DOT/FAA/AR-01/41

Office of Aviation Research
Washington, D.C. 20591

Review of Pending Guidance and Industry Findings on Commercial Off-The-Shelf (COTS) Electronics in Airborne Systems

August 2001

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/AR-01/41		

4. Title and Subtitle	5. Report Date
REVIEW OF PENDING GUIDANCE AND INDUSTRY FINDINGS ON COMMERCIAL OFF-THE-SHELF (COTS) ELECTRONICS IN AIRBORNE SYSTEMS	August 2001
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Robert K. Thornton	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
United Technologies Research Center 411 Silver Lane East Hartford, CT 06108	11. Contract or Grant No. DTFA03-99-C-00030

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Federal Aviation Administration Office of Aviation Research Washington, DC 20591	Final Report
	14. Sponsoring Agency Code AIR-130

15. Supplementary Notes

The FAA William J. Hughes Technical Center COTR was Charles Kilgore. The hyperlinks within this document were current at the time of publication; however, they may or may not function at later dates.

16. Abstract

The intent of this report is to provide findings about the state of the industry relative to the design objectives identified in guidance document DO-254 with focus on the implications for the use of commercial off-the-shelf (COTS) electronic hardware components in safety critical airborne systems. The use of complex electronic hardware components in airborne systems poses a challenge to the meeting of safety requirements because, for complex components, complete verification is, at best, very difficult and, at worst, not achievable. In order to address the potential lack of complete verification, it is recommended that the hardware design life cycle processes should include design assurances to mitigate the possibility that design errors may be introduced into the hardware component and cause anomalous behavior.

New technologies, being developed in the commercial sector, could provide enhanced safety in airborne systems if the technologies could be incorporated at an affordable cost. However, the use of COTS components in airborne systems raises a number of issues with respect to meeting airborne system safety requirements and DO-254 objectives.

Commercial market trends are rapidly diverging from the needs of safety critical airborne systems.

Issues with respect to COTS usage may become barriers in certain cases, if necessary assurances cannot be achieved in a cost effective manner. The assurances required for high criticality applications such as levels A and B will probably not be attainable for COTS components without mitigation by other means.

17. Key Words	18. Distribution Statement
COTS, Software, Electronics, Commercial off-the-shelf, DO-178B, DO-254	This document is available to the public through the National Technical Information Service (NTIS) Springfield, Virginia 22161.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	125	

PREFACE

This report is being submitted to support the Federal Aviation Administration (FAA) contract to United Technologies Research Center on Commercial Off-The-Shelf software and hardware research (COTS).

Radio Technical Commission for Aeronautics (RTCA) Special Committee 180 and EUROCAE Working Group 46 has developed a guidance document RTCA DO-254/EUROCAE ED-80 entitled "Design Assurance for Airborne Electronics Hardware." The document has not yet been adopted by the FAA. The intent of this report is to provide findings about the state of the industry relative to the design objectives identified in DO-254 with focus on the implications for the use of COTS components in safety critical airborne systems.

Industry findings with respect to the usage of COTS components were gathered from conference proceedings, technical and trade journals, and a number of sources available through the World Wide Web.

The report is structured in six sections as follows:

1. Current Role of COTS Hardware in Safety Critical Systems
2. Key Component Attributes Derived From DO-254 Objectives and Guidance
3. Key Attributes of COTS Components in Safety Critical Applications
4. Issues Which Limit the Ability of COTS Components to Meet DO-254 Objective
5. Alternate Methods to Meet DO-254 Objectives With COTS HW
6. Barriers Which Limit the Ability of COTS Components to Meet DO-254 Objectives

1. Current Role of COTS Hardware in Safety Critical Systems

Section 1 of this report provides an overview of the DO-254 guidance, with focus on portions which may be of special interest in the application of COTS components.

Safety critical aircraft functions are being implemented with electronic hardware. Current electronic hardware is moving from simple implementations to more and more complex implementations. This trend generates challenges for the safety and certification of the system. "These challenges arise from a concern that said aircraft functions may be increasingly vulnerable to the adverse effects of hardware design defects that may be increasingly difficult to manage due to the increasing complexity of the hardware" (DO-254, Section 1.0). As the electronics become more complex, the possibility of aircraft design defects increases and adequate verification of the system becomes difficult.

The purpose of DO-254 is to provide guidance in design assurance for the development of airborne hardware such that it "safely performs its intended function, in its specified environments" (DO-254, Section 1.0).

DO-254 addresses the complete hardware design life cycle through a number of processes defined as follows:

DO-254 Hardware Design Life Cycle Processes

- Planning Process
- Hardware Design Processes
  - Requirements Capture Process
  - Conceptual Design Process
  - Detailed Design Process
  - Implementation Process
  - Production Transition Process
  - Acceptance Test
  - Series Production
- Validation Process
- Verification Process
- Configuration Management Process
- Process Assurance
- Certification Liaison Process

DO-254 describes design assurance objectives for airborne electronic hardware, without regard for the source of the components. It is the responsibility of the developer to provide adequate assurance for the component, be it custom designed for the application or COTS.

The use of COTS components will be verified through the overall design process, including the supporting processes, as defined in this document (DO-254, Section 11.2).

Section 1 also provides COTS background through a survey of several definitions for COTS components, the benefits some see in the application of COTS components, and a survey of commercial market trends for electronic components.

While many definitions of COTS components exist in the industry, the DO-254 guidance is concerned with design assurance for safety requirements, irrespective of the components used. While the use of commercially available components will be shown to have several benefits, a significant challenge to the of use of COTS components lies in the fact that, by definition, the component is "developed by a supplier for multiple customers, whose design and configuration is controlled by the supplier's or an industry specification," as found in DO-254 glossary definition of COTS. DO-254 adopts a requirements driven approach in which requirements flow down to the component design, however, for COTS components, the component design is previously established by the COTS component supplier and based on the suppliers perception of the needs of the commercial market targeted by the product.

The COTS development cycle is not in alignment with the DO-254 top-down, requirements-based approach, and it will be seen that this misalignment is the source of issues with respect to the usage of COTS components.

A number of commercial market trends are causing the commercial market to diverge from the needs of critical airborne systems:

- Since the defense industry is now an insignificant portion of the market, other market forces are directing the commercial industry, and are directing it in such a way that new challenges are being created for the critical component sector.

- Product life-time expectations for defense and safety critical airborne systems exceed 20 years, while commercial electronics may become obsolete in 2 to 5 years.

- Production runs for low volume applications, such as defense and safety critical systems, are not economically viable on these production lines.

- Market pressures may move commercial products to trade the perceived excessive end of life reliability for increased performance.

- The rapid introduction of new materials technologies poses a new reliability risk.

- Military and critical airborne systems development processes require COTS vendors to provide services that are beyond those normally required by the commercial sector.

Section 1 includes a discussion of the characteristics of safety critical systems, airborne applications, critical systems in other industries, and the trend toward open system architecture which is expanding the use of COTS components.

The characteristics of safety critical systems include high consequence of failure, high reliability, low volume, operation in harsh environments, and use of complex electronics where the behavior of the system may not be totally predictable by deterministic means.

Also in section 1, findings relative to industry usage of COTS components are presented with focus on three levels of integration: the system/subsystem, the board/module components, and the microelectronic components. Military demonstration programs evidence the most widely accepted application of COTS subsystem/board/module components and open systems architecture, driven primarily by federal mandate. In microelectronics, while all systems are COTS based at some elemental level, the rapid increase in commercial microelectronic complexity is creating a diversion between the needs of commercial and safety critical system markets.

2. Key Component Attributes Derived From DO-254 Objectives and Guidance

The purpose of section 2 is to review the DO-254 objectives and guidance in order to identify attributes, that are required of a component to successfully meet DO-254 objectives. Selected sections of the DO-254 guidance are presented, which are pertinent to components in general

and COTS components in particular. Grouping of the attributes, as described in the Key Attributes Summary, results in the following key component attributes:

- Design Assurance
- Component Reliability
- Standards
- Failure Modes
- Operation Beyond Mfg. Spec.
- Upsets
- Service Experience
- Configuration Management
- Production Practices
- Verification Testing
- Role of COTS Tools in Design and Verification

3. Key Attributes of COTS Components in Safety Critical Applications

Component Reliability

Evaluation of the reliability practices of a significant number of commercial companies lead to several key observations which include the following:

- Thoroughly understanding the design is essential to reliability.

- Strong supplier relationships are essential.

- Military standards, in many cases, form the basis of commercial reliability practices; however, they are often revised or modified for internal use.

- Military specifications and standards, if used without regard to their applicability or value-added, can drive up costs with no positive affect on reliability.

- Only DoD is doing and funding research needed to develop technical information included in military standards and making it available to industry. If and when commercial companies perform such research, the results are usually kept proprietary.

- Designing for reliability must include the reliability of the processes as well as the product.

- Parts application is critical—select the parts most appropriate for the design and stress levels.

This evaluation was found in "Benchmarking Commercial Reliability Practices."

Use of Standards

DO-254 provides guidance relative to using standards in the hardware design life cycle; however, it does not specify particular standards. The adoption of standards seems to be left to the applicant.

The DoD is reforming the Military Specification program through migration to commercial standards where appropriate. DoD is shifting focus from "how to do it" specifications to performance requirements. While the migration to performance requirements enables the use of technology in new ways, it also moves the burden of responsibility directly to the system provider/designer. Previously, the designer could have confidence that the Mil-Spec part would perform reliably in harsh environments. "In the absence of Mil-Specs, a designer must determine the environment in which the electronic system will operate, establish that a particular commercial Integrated Circuit (IC) will operate reliably in that environment, and plan for parts obsolescence," in "Overcoming Barriers to the Use of Commercial Integrated Circuit Technology in Defense Systems." The designer now must establish in-house standards and also evaluate the in-house and industry standards which may be used by suppliers.

Failure Modes

Next generation microelectronics may exhibit new failure modes brought about by several technology trends being pursued to increase the performance/cost ratio of the devices.

Operation Beyond Manufacturers Specifications

Components are "uprated" by the Original Equipment Manufacturers (OEMs) who employ extra testing and part screening to establish that components have extra margins that allow operation at higher temperatures, under radiation conditions, or other conditions which may be required for critical applications. OEMs may invest significant effort in qualifying COTS components for uprated operation. The OEM must implement a strategy to address supplier process changes or variations which may impact the characteristics which have been qualified. Supplier agreements and extensive unit tests are two approaches.

Single Event Upsets

The rapidly changing technologies of the commercial sector, coupled with the disappearance of suppliers for radiation-hardened devices, provide significant challenges. Device scaling effects, driven by commercial market pressures, "often result in increased vulnerability to radiation. ...the introduction of new and emerging technologies that promise greater performance without increased power, weight, or volume may have completely unknown radiation effects behavior that must be established through testing," in "Recent Radiation Effects Activities at JPL: Coping With COTS."

Product Service Experience (PSE)

PSE may be an important assurance strategy for COTS components in some applications. In the DoD's transition to COTS components, a number of military demonstration programs are being conducted which may help establish PSE.

DeBusk, in "Managing the Reliability of COTS-Based Military Systems," claims "The cornerstone of COTS predictions are observed equipment mean time between failures (MTBFs)... measuring the observed MTBF is the only way to accurately assess the reliability of COTS equipment in military environments."

Production Practices

IC manufacturers processes were improved, over the last 10 years, such that occurrence of defective components has been reduced to as low as 100 ppm. Some OEMs are therefore eliminating the costly in-house part screening tests and instead, establishing supplier qualification programs. The OEMs approve suppliers who demonstrate the manufacturing processes necessary to reliably provide defect-free parts.

Configuration Management

Approaches to dealing with parts obsolescence are expensive and cumbersome. They include stock piling of original parts, transfer of technology and tooling to third-party suppliers, re-engineering of the obsolete microcircuit, or redesign of parts or all of the subsystem.

Configuration management and change impact assessment may become issues if changes, which occur in COTS components, impact safety requirements. The design processes and assurances impacted by any change must be evaluated to determine if the change effects the ability to meet the safety requirements.

Verification Approaches

For critical applications, the tradeoff between testing at the COTS supplier and testing at the OEM is a challenging issue, which is becoming more important as microelectronics become more complex.

The effectiveness of testing techniques currently in use will be challenged as the industry moves to smaller scale devices and new packaging techniques.

Role of COTS Tools in Verification Analysis

The current move towards System On a Chip (SOC) designs, which may incorporate close to one million gates, has sparked the development of a new wave of Electronic Design Automation (EDA) tools which will enable the trend towards more complex commercial microelectronics. While qualification of these tools is an issue, the new tools may provide some increased level of design assurance.

4. Issues Which Limit the Ability of COTS Components to Meet DO-254 Objectives

Section 4 reviews the key component attributes, identified in section 2, with respect to issues which limit the ability of COTS components to provide these key attributes and to thus meet DO-254 objectives.

Summary of Identified Issues
Which Limit the Ability of COTS Components to Meet DO-254 Objectives

Design Assurance

Issue: "Actual availability of COTS component design assurance data as required by" DO-254, Section 11.2.2.

Component Reliability

Issue: Actual availability of COTS component data as required to determine failure rates by an acceptable method.

Standards

Issue: Standards for electronics development and production are diverse, do not address the needs of critical systems, and are no longer supported by the federal government.

Failure Modes

Issue: It may be difficult to identify all fault modes, i.e., anomalous behavior, for complex COTS components.

Operation Beyond Manufacturer's Specification and Upsets

Issue: COTS component suppliers discourage use of their components in unintended environments

Issue: The manufacturer specified operating range of COTS components do not meet the requirements for many airborne applications

Issue: COTS components may exhibit anomalous behavior due to Electromagnetic Interference (EMI) and radiation.

Service Experience

Issue: The quality of COTS service experience data may be inadequate to meet safety requirements.

Configuration Management and Production Practices

Issue: COTS suppliers are at liberty to change their production processes

Issue: COTS suppliers are at liberty to discontinue production of a component resulting in "COTS components which become non-procurable" DO-254, Section 11.2.2.

Issue: "Variations in component parameters that depend on production batches may not be identified, even by robustness tests," DO-254, Section 11.2.2

Issue: "Evolving aspects of electronic component technology," DO-254, Section 11.2.2

Issue: Quality control provided by COTS suppliers may be inadequate.

Verification Testing

Issue: Production testing done by COTS suppliers may fail to detect defective components.

Issue: OEMs may not have sufficient design information or resources to adequately test complex COTS components.

Role of COTS Tools in Design and Verification

Issue: Design tools used by both COTS suppliers and OEMs may introduce design errors.

Issue: Verification tools used by both COTS suppliers and OEMs may fail to identify defective components.

5. Alternate Methods to Meet DO-254 Objectives With COTS Hardware (HW)

Section 5 provides findings, in selected areas, of alternate methods to meet DO-254 objectives with COTS hardware.

Design Assurance—Advanced Electronic Design Automation (EDA)

While complex ICs reduce unit cost by packing more functionality into smaller die sizes, the development costs must be controlled by using design methods that result in a successful prototype on the first attempt. Design challenges are being faced in many areas including timing analysis, power consumption, cross-talk, metal migration, and power distribution within the IC. New EDA tool developments will allow commercial designers to address the design challenges earlier in the design process, providing additional design assurance that was previously unattainable. While qualification of these tools is an issue, the new tools may provide some increased level of design assurance.

Component Reliability—Prediction

Empirically based reliability prediction methods, and in particular MIL-HDBK-217, have been criticized for the following shortcomings identified in "Evaluating the Reliability of COTS Items":

- Method is not a good indicator of field reliability
- Temperature cycling is not accounted for
- Method does not reflect new manufacturing trends
- Method does not differentiate good quality and design practices
- System level factors that influence reliability are penalized (e.g., transient protection circuits)
- Method is not "science based"

"Physics-of-failure methods predict when a single specific failure mechanism will occur for an individual component due to wear out (end-of-life)," as stated in "Evaluating the Reliability of COTS Items." A component may have numerous failure mechanisms and the model for each requires component specific, detailed knowledge of geometry and materials.

"Evaluating the Reliability of COTS Items," provides the following recommendations for appropriate use of empirical and physics-of-failure methods:

Use Empirical Methods:

- When reliability estimates are performed for large, complex products
- When reliability estimates are developed on a quick-turnaround basis
- When there is a need to estimate the relative merits of competing designs
- When there is no way to change the fundamental design of the components
- When the only design flexibility is to select different components or limit applied component stresses

Use Physics-of-Failure Methods:

- When a detailed understanding of life-limiting failure mechanisms is needed
- When new component technologies need to be assessed and no historical data exists
- For detailed component design prior to life testing and qualification
- When design flexibility exists at the component level
- To investigate the root cause of a failure

Physics-of-failure models are the basis of handbook predictions and design rules used in EDA tools for IC silicon layout. Electron migration is an example of a wear out type failure mechanism, which physics of failure predicts, based on chip geometry. For submicron geometries in commercial applications, the designer can tradeoff useful lifetime for added functionality, resulting in failure due to wear-out mechanisms after, say 5 years, instead of the traditional goal of 10 to 15 years. For commercial applications, a 5-year lifetime may be more than adequate in some markets. Knowledge of the design rules and target lifetime for COTS components may soon become an issue in safety critical applications.

PRISM is a software tool for estimating the failure rate of electronics systems, based on a new methodology developed by the Reliability Analysis Center (RAC). Both component reliability prediction models and methods to assess the impact of noncomponent variables, on system reliability, are provided. RAC developed the system assessment methodology to overcome some of the perceived limitations of MIL-HDBK-217. "The purpose of PRISM is to provide an engineering tool to assess the reliability of electronic systems. It is not intended to be the "standard" prediction methodology, and it can be misused if applied carelessly," as stated in the "Journal of the Reliability Analysis Center."

The limitations of reliability models should be considered when using them for reliability prediction methods. Twelve common microcircuit reliability models have been examined and shown to have shortcomings. Physics-of-failure model development is targeted at addressing model shortcomings identified, however, detailed design information is clearly required to assess the mechanisms at this level of detail.

Operation Beyond Manufacturers Specifications

The International Electrotechnical Commission (IEC) has produced a guidance document for the qualification of components for operation beyond the manufacturers specified temperature range; "Avionics Industry: Guide for Using Semiconductor Devices Outside Manufacturers Specified Temperature Ranges." The practice is specifically discouraged, but it is recognized that in some cases there is no alternative.

"Component stress balancing consists of operating the component at a temperature above that specified by the component manufacturer; and compensating by reducing at least one of the other operating parameters, e.g., power, speed, to the extent that the junction temperature remains below its maximum rating, with acceptable specified margin," as stated in the Avionics Industry document.

Cocooning is an approach which regulates the environment seen by the component, such that the manufacturers specified environment is maintained. Cocooning has been used successfully in military applications of COTS components, especially board level components; however, the cost of the cocooning provisions can be significant.

Upsets

Government-sponsored device characterization programs are the primary source of advancement in this area.

Configuration Management

Parts obsolescence will persist as a problem for OEMs serving markets that require supported lifetimes of 20 years or more. Commercial market trends will make parts obsolescence even more significant in the future. Alternate methods currently employed to mitigate parts obsolescence are all very costly. It remains to be seen, if the current COTS trend in military programs can be supported at reasonable cost over the life of the systems.

Verification Testing: Production Testing Techniques

Testing of complex ICs will require the use of several test methods which should include both structural testing and functional testing. Structural testing attempts to verify that the device elements function, according to the silicon design, without defect in transistors or interconnects. Structural testing assumes that the silicon design will properly implement the intended function, therefore, if the device elements properly execute the silicon design, then the intended functions will operate properly. Functional testing attempts to verify that the device will perform its intended function.

The issue of adequate test coverage remains a challenge, which is of particular importance to safety critical applications.

Role of COTS Tools in Design and Verification

As the complexity of commercial electronic components increases, the design, verification of design, and production testing are becoming increasingly dependant on EDA tools. In addition, commercial pressures dictate that the layout of the chip be free of design errors on the first attempt. EDA tools are evolving to meet the need for design verification during the commercial design process. New tools are addressing sources of design errors which were previously only discovered during evaluation of the silicon. While qualification of these tools is an issue, the new tools may provide some increased level of design assurance.

6. Barriers Which Limit the Ability of COTS Components to Meet DO-254 Objectives

Section 6 discusses issues which may present barriers to the ability of COTS components to meet DO-254 objectives.

COTS component usage in safety critical applications requires significant OEM development effort targeted at the COTS component and COTS supplier cooperative efforts. While DO-254 treats COTS components as previously designed hardware, the hardware life cycle processes and objectives are applicable to any type of hardware, not precluding COTS usage, but holding all hardware to the same assurance standards. Therefore, while DO-254 objectives do not present barriers to COTS usage, the level of development effort required by the OEM may be cost-prohibitive to COTS usage as compared to custom hardware designs. Alternative methods, which attempt to address the issues, are in use throughout the industry; however, the cost of the alternative methods may be prohibitive in some applications.

Levels A and B assurances obviously pose the greatest challenge to the viable use of COTS components due to the development effort required by the OEM to meet assurance objectives. While the objectives do not constitute barriers, the cost of adequate assurance development may well be a barrier to COTS usage for applications of levels A and B criticality.

The benefits in additional functionality, which might be achieved through the use of low-cost COTS components, will be achievable in airborne applications, only if the development effort/cost required for assurances can be secured in a cost-effective manner. Adequate assurances and evidence are achieved at a cost incurred by the OEM and their customers. If the required assurances and evidence, once achieved, could be reused in other applications, the cost could be distributed over a larger population of systems, thus reducing the cost per system. Open systems, reusable designs, and certifiable COTS components with industrywide shared evidence and assurances may be required to gain the functional benefits of COTS components.

TABLE OF CONTENTS

		Page
EXECUTIVE SUMMARY		xxi
1.	CURRENT ROLE OF COTS HARDWARE IN SAFETY CRITICAL SYSTEMS	1
1.1	Overview of Pending Guidance	1
1.1.1	Hardware Complexity	1
1.1.2	Hardware Design Life Cycle Processes	2
1.1.3	System Design/ HWDLC Data Exchange	2
1.1.4	Hardware Design Assurance Level	3
1.1.5	Hardware Safety Requirements	3
1.1.6	Data Requirements	5
1.2	COTS Background	6
1.2.1	Defining COTS	6
1.2.2	Motivations to Employ COTS Components	8
1.2.3	COTS Market Trends	9
1.2.4	Consortium Research	12
1.3	Areas of Application for Safety Critical and COTS Components	12
1.3.1	Characteristics of Safety Critical Applications	12
1.3.2	Airborne Applications	13
1.3.3	Applications in Other Industries	14
1.3.4	Open System Application Trends	16
1.4	Types of Components in Use	17
1.4.1	System/Subsystem Components	17
1.4.2	Board/Module Components	20
1.4.3	Microelectronics Components	21
2.	KEY COMPONENT ATTRIBUTES DERIVED FROM DO-254 OBJECTIVES AND GUIDANCE	23
2.1	COTS Component Usage and Procurement	23
2.2	Hardware Safety Assessment (HSA)	24
2.2.1	Hardware Safety Assessment and Hardware Design Assurance Level	24
2.2.2	Design Assurance Strategy	25
2.2.3	Design Assurance Methods	26
2.3	Hardware Planning Process	27

2.4 Hardware Design Process (HDP)—Requirements Capture and Conceptual Design Objectives 28

2.4.1 Hardware Design Process—Requirements Capture Objectives 28
2.4.2 Hardware Design Process—Conceptual Design Objectives 29

2.5 Hardware Design Process—Detailed Design Process Objectives 29

2.6 Hardware Design Process—Implementation Process Objectives 29

2.7 Hardware Design Process—Production Transition Objectives 30

2.8 Validation Process Objectives 30

2.9 Verification Process Objectives 30

2.10 Configuration Management Process Objectives 32

2.11 Process Assurance Objectives and Certification Liaison Process Objectives 34

2.12 Standards 34

2.13 Electronic Component Management Process 34

2.14 Tool Assessment and Qualification 35

2.15 DO-254 Appendix A—Modulation of Hardware Life Cycle Data Based on Hardware Design Assurance Level 36

2.16 Key Attributes Summary 36

3. KEY ATTRIBUTES OF COTS COMPONENTS IN SAFETY CRITICAL APPLICATIONS 37

3.1 Pending Guidance on COTS Components 37
3.2 Component Reliability 39

3.2.1 Reliability Metrics Overview 39
3.2.2 Benchmarking Commercial Reliability Practices 39
3.2.3 Tools for COTS Equipment Reliability Assessment 41
3.2.4 Military Demonstration Programs 42
3.2.5 Packaging Trends 43

3.3 Use of Standards 43

3.3.1 Standards: Safety Verification/Validation 45
3.3.2 Quality Manufacturers List 46

3.4 Failure Modes 48
3.5 Operation Beyond Manufacturers Specifications 48

3.6 Single-Event Upsets 49
3.7 Product Service Experience 50
3.8 Production Practices 50

3.8.1 Review of Best Manufacturing Practices 50
3.8.2 Review of Quality and Reliability Programs 52

3.9 Configuration Management 52

3.9.1 Pending Guidance on Configuration Management 52
3.9.2 Parts Obsolescence 53

3.10 Verification Approaches 54

3.10.1 DO-254 Pending Guidance for Verification 54
3.10.2 Verification Testing 55

3.11 Role of COTS Tools in Verification Analysis 58

3.11.1 DO-254 Pending Guidance for Analysis and Simulation 58
3.11.2 DO-254 Pending Guidance for Tools 58
3.11.3 Another Guidance Discussion on Tools 59
3.11.4 Overview of the Role of Tools in Design and Verification 60

4. ISSUES WHICH LIMIT THE ABILITY OF COTS COMPONENTS TO MEET DO-254 OBJECTIVES 62

4.1 Design Assurance 62
4.2 Component Reliability 63
4.3 Standards 63
4.4 Failure Modes 64
4.5 Operation Beyond Manufacturer's Specification and Upsets 64
4.6 Service Experience 64
4.7 Configuration Management and Production Practices 65
4.8 Verification Testing 65
4.9 Role of COTS Tools in Design and Verification 66
4.10 Summary of Identified Issue 66

5. ALTERNATE METHODS TO MEET DO-254 OBJECTIVES WITH COTS HARDWARE (HW) 67

5.1 Advanced Electronic Design Automation 67

5.1.1 Electronic Design Automation Overview 67
5.1.2 Timing Analysis 69
5.1.3 Power Supply Network 69
5.1.4 Electromigration (EM) 69
5.1.5 Unifying Language 69

5.1.6 Emulation 70
5.1.7 Simulation 70
5.1.8 Model Checking 70
5.1.9 Crosstalk 70

5.2 Approaches to Mitigate Undeclared, Unused Additional Functions (UUAF) 71
5.3 Component Reliability 71

5.3.1 Empirical Models for Reliability Prediction 71
5.3.2 Similarity Analysis 72
5.3.3 Physics of Failure 73
5.3.4 Field Data Analysis 75
5.3.5 PRISM Reliability Assessment Methodology 76
5.3.6 Reliability Model Assessment 78
5.3.7 Activation Energy-Based Testing Assumptions 79

5.4 Failure Modes 79
5.5 Operation Beyond Manufacturer's Specifications 80

5.5.1 International Electrotechnical Commission (IEC) Guidelines 80
5.5.2 Component Stress Balancing Method 80
5.5.3 Cocooning 81

5.6 Upsets 81
5.7 Configuration Management 82

5.7.1 Mitigating Parts Obsolescence 82
5.7.2 Technology Insertion 83
5.7.3 Wafer Banking 83

5.8 Verification Testing: Production Testing Techniques 83

5.8.1 Built-In Self-Test (BIST) and Structural Testing 84
5.8.2 Automatic Test Equipment and Functional Testing 85
5.8.3 Virtual Test Software 85
5.8.4 Environmental Testing Approaches 85

5.9 Role of COTS Tools in Design and Verification 85

6. BARRIERS WHICH LIMIT THE ABILITY OF COTS COMPONENTS TO MEET DO-254 OBJECTIVES 86

6.1 Issues and Barriers 87
6.2 Conclusions 89

7. REFERENCES 90

8. RELATED RESOURCES 96

LIST OF TABLES

Table		Page
1	DO-254 Hardware Design Life Cycle Processes	2
2	Selected CALCE Members	12
3	Key Component Attributes	37
4	Specification Transition—From Military to *Almost* Equivalent Commercial	45
5	QML Manufacturers per QML 38535 rev 012	47

EXECUTIVE SUMMARY

The contract for this research is summarized below under the heading of Hardware and Software. There are two final deliverables, one technical report on hardware COTS components and one technical report on software COTS components.

HARDWARE

This report is being submitted to support the Federal Aviation Administration (FAA) hardware portion of the contract to United Technologies Research Center on Commercial Off-The-Shelf (COTS) software and hardware research.

The intent of this report is to provide findings about the state of the industry relative to the design objectives identified in guidance document entitled "Design Assurance for Airborne Electronics Hardware" (DO-254), with focus on the implications for the use of COTS electronic hardware components in safety critical airborne systems. Industry findings were gathered from conference proceedings, technical and trade journals, and a number of sources available through the World Wide Web.

The use of complex electronic hardware components in airborne systems poses a challenge to the meeting of safety requirements because, for complex components, complete verification is, at best, very difficult, and at worst, not achievable. In order to address the potential lack of complete verification, it is recommended that the hardware design life cycle processes should include design assurances to mitigate the possibility that design errors may be introduced into the hardware component and cause anomalous behavior.

New technologies, being developed in the commercial sector, could provide enhanced safety in airborne systems if the technologies could be incorporated at an affordable cost. However, the use of COTS components in airborne systems raises a number of issues with respect to meeting airborne system safety requirements and DO-254 objectives.

Commercial market trends are rapidly diverging from the needs of safety critical airborne systems.

Key component attributes have been identified as desirable/necessary to meet design objectives. Key component attributes include design assurance, component reliability, operation beyond manufacturer specifications, service experience, configuration management, production practices, verification testing, and role of COTS tools in design and verification. COTS components are challenged to provide many of these attributes. Therefore, the ability of COTS components to meet the DO-254 design objectives may be limited by a number of issues, which are explored in this report.

Successful application of COTS components, in airborne systems, requires extensive Original Equipment Manufacturer (OEM) effort to develop the required assurances for the COTS component. In addition, design assistance needs to be extended to the OEM, by the COTS supplier, which is well beyond that which is normally provided in the commercial sector. If the COTS supplier is unable or unwilling to provide necessary design information for a certain COTS component, then the OEM effort associated with developing design assurances will be significantly increased and may preclude the use of the COTS component.

Issues with respect to COTS usage may become barriers in certain cases, if necessary assurances cannot be achieved in a cost-effective manner. The assurances required for high criticality applications, such as levels A and B, will probably not be attainable for COTS components without mitigation by other means.

The contract for this research included two final report deliverables: this report which is related to COTS hardware components, and a report on COTS software components identified in the FAA report "Commercial Off-The-Shelf (COTS) Avionics Software Study," DOT/FAA/AR-01/26, May 2001. The executive summary of the software report is presented, in this hardware report, at the request of the sponsoring agency, to brief readers on the contract work relating to software.

SOFTWARE

Typical COTS software components are utilized in low-risk applications and many have been developed without considering the safety aspects of the software. However, to utilize this software in airborne systems requires that the COTS product be scrutinized to determine its ability to meet the intent of Radio Technical Commission for Aeronautics (RTCA) Inc., document "Software Considerations in Airborne Systems and Equipment Certification," DO-178B objectives. The ability to access a COTS product's development and product verification documentation, if any was produced, is usually limited. However, some products are being developed specifically for the airborne market, albeit the selection is limited, it is growing.

Issues concerning the usage of COTS are not completely addressed in DO-178B. Due to the current relationship with the vendor, the avionics application represents efforts on behalf of both parties. Thus, problem reporting, COTS prior operation environment, version control, and process and product examination requires special attention. Some domains using COTS have considered a separate COTS specific process plan to analyze the safety, integration and verification aspects of the COTS components, and the overall avionics application.

Operating systems are currently receiving the most attention, and several real-time operating system vendors have commenced efforts to provide "DO-178B ready" COTS operating systems. A variety of hardware and software architectural techniques exist to reduce the risk of using COTS components in avionics and other domains. Furthermore, verification techniques and other alternative methods are being applied in combination on the COTS component in efforts to meet the "intent of DO-178B". The more popular techniques currently being used include reverse engineering of the COTS component, software protection wrappers, partitioning, and COTS component service history. Some COTS operating system vendors are paying particular attention to how their component is being integrated into the avionics product and provide a variety of data and services to support this integration.

A detailed review of DO-178B's objectives identifies which objectives are providing resistance to COTS technology insertion. This level-dependent review shows that many typical COTS components are more applicable to the software levels C and D avionics applications and, that the DO-178B levels A and B objectives relating to strict structural testing and independence make COTS utilization more difficult. The details of this effort are found in the FAA "Commercial Off-The-Shelf (COTS) Avionics Software Study" report.

1. CURRENT ROLE OF COTS HARDWARE IN SAFETY CRITICAL SYSTEMS.

1.1 OVERVIEW OF PENDING GUIDANCE.

Safety critical aircraft functions are being implemented with electronic hardware. Current electronic hardware is moving from simple implementations to more and more complex implementations. This trend generates challenges for the safety and certification of the system. "These challenges arise from a concern that said aircraft functions may be increasingly vulnerable to the adverse effects of hardware design defects that may be increasingly difficult to manage due to the increasing complexity of the hardware" (see section 1.0 of reference 1). As the electronics become more complex, the possibility of aircraft design defects increases and adequate verification of the system becomes difficult.

The purpose of DO-254 is to provide guidance in design assurance for the development of airborne hardware such that it "safely performs its intended function, in its specified environments." The document defines assurance objectives and their basis. The objectives are described to allow the development of means of compliance with guidance that is appropriate to the system. DO-254 also provides guidance for design assurance activities to meet the design assurance objectives. The guidance is intended to be flexible with respect to the processes, which the design adopts to meet the design assurance objectives and allows for the use of improved processes in the future (see section 2.3.1 of reference). Focus seems to be on defining the desired performance of the system, rather than prescribing "how to" specifications to achieve the desired performance.

1.1.1 Hardware Complexity.

> "*...the feasibility and level of difficulty necessary to accomplish acceptable verification coverage by deterministic means...*" *(see section 1.6 of reference 1) is the basis for defining the complexity of the hardware item. "A hardware item is identified as simple only if a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior*" (see section 1.6 of reference 1).

A hardware item is classified as complex if it cannot meet the criteria for a simple item. Deterministic verification may not be practical or even possible for complex items. Some functions may not be testable such as unused functions or potential hidden states of sequential machines. All foreseeable operational and abnormal behaviors may be difficult or impossible to identify for complex items.

The design assurance level needed for safety functions must be achieved by the proposed hardware item, be it simple or complex. Use of complex items may require additional design requirements in areas of, for example, design architecture to meet the design assurance level needed for the function.

1.1.2 Hardware Design Life Cycle Processes.

The DO-254 guidance is concerned with processes associated with the Hardware Design Life Cycle (HWDLC). These processes are shown in table 1.

TABLE 1. DO-254 HARDWARE DESIGN LIFE CYCLE PROCESSES

• Planning Process
• Hardware Design Processes
- Requirements Capture Process
- Conceptual Design Process
- Detailed Design Process
- Implementation Process
- Production Transition Process
- Acceptance Test
- Series Production
• Validation Process
• Verification Process
• Configuration Management Process
• Process Assurance
• Certification Liaison Process

1.1.3 System Design/ HWDLC Data Exchange.

The system design process provides information to the HWDLC process as described completely in section 2.1.1 of reference 1. Selected information defined by the system design process includes:

- The design and safety requirements allocated to the hardware
- The design assurance level for each function
- Allocated probabilities and at-risk exposure times for hardware function failures
- Environmental requirements allocated to the hardware.

This information defines the design assurance level and operating conditions for the hardware in terms of hardware requirements which must be met and verified.

The HWDLC process provides information back to the system design process as detailed in section 2.1.2 of reference 1. This information includes safety analysis data such as:

- Probability and failure rates for designated hardware functional failures
- Common mode fault analysis
- Isolation boundaries and generic fault mitigation strategies

Systems, which incorporate COTS components, may be challenged to provide adequate approaches to satisfying the information data requirements. Novel approaches to architecture for isolation boundaries and fault mitigation strategies may be required.

1.1.4 Hardware Design Assurance Level.

Table 2-1 of reference 1, defines the Hardware Design Assurance Level associated with the five levels of safety criticality: Levels A–E.

- Level A is most critical, with a classification for failure condition of "catastrophic", i.e., "Failure conditions that would prevent continued safe flight and landing." While effects on occupants are not defined for this level, fatal injury to many of the occupants would probably result.

- Level B failure conditions could result in serious or potentially fatal injuries to a small number of occupants.

- Level C failure conditions could result in discomfort or injuries.

- Level D failure conditions could result in inconvenience.

- Level E failure conditions have no effect on occupants.

The probability of failure associated with safety functions is discussed in reference 2, based on FAR section 25.1309 of part 25, subsequent to amendment 25-23. Allowable risk is defined in the context of 1 hour of flight time based on a flight of mean duration for the aircraft type. Critical functions have probability of failure 1×10^{-9} or less. Essential functions have probability of failure 1×10^{-5} to 1×10^{-9}. Nonessential functions have probability of failure 1×10^{-5} or greater. This would indicate that the most critical safety functions, level A and possibly level B, require probability of failure of 1×10^{-9} or less. Critical functions are characterized as extremely improbable events so unlikely that they need not be considered to ever occur. Reference 2 points out that, for a posed example of 100 parts in series, the time to first failure would be ~ 3×10^{4} unit-hrs, which would require over 3 1/2 years to verify through field data. Accelerated bench testing of a dual redundant system would require only 2 weeks of testing to demonstrate this level of reliability, however, the extent to which all pertinent operating stresses are addressed in accelerated testing is a concern.

Failures of essential functions are considered unlikely to occur during the total operational life of a single airplane of a particular type, but may occur during the total operational life of all airplanes of a particular type.

Failures of nonessential functions may be expected to occur during the life of each airplane.

1.1.5 Hardware Safety Requirements.

The hardware safety assessment is an iterative process with the hardware design that helps determine the hardware safety requirements and ensures that the safety requirements allocated to the hardware are satisfied. The derived requirements (see section 2.3.1 of reference 1) for the hardware include:

"...safety requirements for hardware architecture, circuits and components, and protection against anomalous behaviors, including incorporating specific hardware architectural and functional safety attributes such as:

Circuit or component redundancy.
Separation or electrical isolation between circuits or components.
Dissimilarity between circuits or components.
Monitoring of circuits or components.
Protection or reconfiguration mechanisms.
Allowed failure rates and probabilities for circuit and component random failures and latent failures.
Limitations of usage or installation.
Prevention and management of upsets and upset recovery"

"The hardware design assurance process and the hardware safety assessment should jointly determine the specific means of compliance and design assurance level for each function and should determine that an acceptable level of design assurance has been achieved."

The amount of design assurance necessary to ensure that related failure conditions have been mitigated increases as the severity level of the failure condition increases. The design assurance considerations for levels A and B functions should address potential anomalous behaviors and potential design errors. "The design assurance strategy should be selected as a function of the hardware architecture and usage and of the hardware implementation technology that has been chosen" (see section 2.3.4 of reference 1).

DO-254 notes that there are two types of anomalous behavior of the hardware which are assessed using various qualitative and quantitative assessment methods.

The first type of anomalous behavior, random faults, may be assessed through quantitative means, including "Statistical failure assessment and prediction methods, which are based on hardware failure rates, redundancy, separation and isolation, failure mode statistics, probability analysis, component de-rating, stress analysis, and manufacturing process control" (see section 2.3.2 of reference 1).

The second type of anomalous behavior includes design errors in a hardware item and upsets to the hardware. "Unlike random failures of hardware, neither design errors nor some types of upsets are statistically predictable, and both may cross redundancy boundaries in the form of common mode faults. Redundancy management techniques and quantitative assessment methods to be used should be selected so that potential common mode faults and the effects of upsets are precluded or mitigated when necessary. Although difficult to assess quantitatively, safety risk from design errors and upsets can be effectively assessed by a practical application of qualitative safety assessment methods. Analysis techniques, such as fault tree analysis, common mode analysis, and functional failure modes and effects analysis (F-FMEA), are fundamentally qualitative methods, and can be used to address hardware design errors and upsets" (see section 2.33 of reference 1).

1.1.6 Data Requirements.

Section 10 of reference 1 describes the data that should be produced during the design cycle. Since the availability of adequate design data is a concern for COTS implementations, guidance for selected data requirements from section 10 are extracted below. Note the entire text of DO-254 should be reviewed for other applicable considerations.

Section 10.1 of reference 1 describes six planning documents to be developed by the applicant. These planning documents provide an important mechanism for communicating the intent of the applicant to the certification authorities. Two of the planning documents require special attention for COTS components.

The Plan for Hardware Aspects of Certification (PHAC) "defines the processes, procedures, methods and standards to be used to achieve the objectives of this document and obtain certification authority approval for certification of the system containing hardware items" (see section 10.1.1 of reference 1). This plan should include, for each function of the hardware item, a description of potential hardware failure conditions; the hardware design assurance level assigned, with justification via safety assessment; and the proposed means of compliance. The plan should identify COTS usage and tool assessment and qualification as appropriate.

In some cases, it may be difficult to adequately identify the hardware failure conditions for COTS components. Architecture, fault tolerant, redundancy, and partitioning are some design techniques which may be employed to mitigate uncertainties with respect to COTS components, and these techniques should be identified in the PHAC if used to assure that the safety requirements are met.

The Hardware Design Plan (see section 10.1.2 of reference 1) should include description of the "... detailed design methods, synthesis techniques, implementation methods, ..." and design tools used. This type of information may be difficult to obtain from the COTS developer for COTS components. Design data, which will be provided for the hardware item, must be identified as well as the source of the design data, be it produced during the design process or previously developed as in the case of COTS components.

The applicant must identify the hardware requirements which have been formulated for the hardware item as described in section 10.3.1 of reference 1. The requirements include "hardware reliability and quality requirements, including requirements related to failure rates, exposure times, and design constraints." Prediction of failure rates for COTS components, particularly board level assemblies, may be challenging and require a cooperative effort with the COTS component supplier or extensive reverse engineering efforts.

"The conceptual design data is the data that describes the hardware item's architecture and functional design..." (see section 10.3.2.1 of reference 1). Conceptual design data should address important airworthiness considerations such as electromagnetic interference (EMI), lightning, shock and vibration, and unused functions in major components. If the COTS component is to be employed outside it's specified operating environment, additional testing may be required to achieve adequate assurance. The issue of the impact of unused functions must be resolved.

"The detailed design data describes the data necessary to implement the hardware item consistently with its requirements. Depending on the hierarchical level of the hardware item, this may include .... HDL hardware description, reliability data, test methodology data, list of unused functions in selected components and actions taken to assure they will not compromise the safety of the hardware item..." (see section 10.3.2.2 of reference 1). Again, when using of COTS components, procuring the data described above may be challenging.

1.2 COTS BACKGROUND.

1.2.1 Defining COTS.

A variety of definitions for COTS components exists in the industry. Much attention has been associated with COTS components since the DoD initiative, in 1994, to promote the use of COTS components—The Federal Acquisition and Streamlining Act of 1994. Much confusion exists in the industry and media, as vendors scramble to promote use of their COTS components.

DO-254 defines COTS in the glossary of terms as follows:

> *"Commercial Off-The-Shelf (COTS) Component-Component, integrated circuit, or sub-system developed by a supplier for multiple customers, whose design and configuration is controlled by the supplier's or an industry specification.*
> *Note: Examples of COTS components may include resistors, capacitors, microprocessors, un-programmed Field Programmable Gate Array and Erasable Programmable Logic Devices, other integrated circuit types and their implementable models, printed wiring assemblies and complete LRUs which are typically available from a supplier as a catalog item."*

By this definition, the component is developed by the supplier and the design is controlled by the supplier. With COTS components, requirements do not flow from the customer to the supplier, but rather the supplier both develops and supplies a component which performs in a way which the supplier judges as desirable for the market segment in which the supplier wishes to make profit.

DY 4 Systems is one of many vendors who supply COTS computer boards to the defense industry. They suggest the following definition for COTS. [3]

Perhaps three simple rules to define COTS are appropriate.

- The product is offered for sale, from a catalog and a price list, by the vendor who has developed and is sustaining the product at his own expense.
- The product conforms to an industry standard which by definition has other vendors also adopting and following the same standard.
- The product was not developed using government funds or is currently no longer owned or maintained by the government.

Emphasis here is placed on development at the vendor's expense and on compliance to a selected industry standard for interfacing with other system components. Vendors in these markets work closely with the customer during the design phase of the program. In this relationship, the customer requirements may flow into the design process, further clouding the definition of COTS.

Reference 4 offers a government perspective on the definition of COTS as follows:

> *"COTS—Components, modules, systems, or software traded in the course of normal business operations at prices based on established catalogue or market prices."*

Federal Acquisition Regulations (FAR) recognize three grades of COTS components [4].

- Commercial grade (0° to +70°C) components
- Industrial grade (-40° to +85°C) components
- Standard Microcircuit Drawing (SMD), Qualified Manufacturers List (QML) (-55° to +125°C), and avionics grade microcircuit.

SMD/QML microcircuits are said to meet all FAR criteria for commercial microcircuits since they are listed in supplier's catalogs, have established prices and specifications, and are sold to the general public.

The "COTS module" applies to the general trend of military equipment suppliers to employ commercially available products. Three categories of equipment can be defined by operating environment [4].

- Benign—commercial, office
- Relatively harsh—industrial
- Harsh—Mil-Spec grade

Vendors are offering products for all three operating environments, sometimes referred to as "ruggedized".

Reference 5 describes definitions of commercial and modified commercial items based on FAR 2.101 and DoD 5000.2R, as applied to submarine COTS acquisition policy.

- Commercial Item

> *"A commercial item is defined as any item, other than real property, that is of a type customarily used for nongovernmental purposes and that:*
>
> *1. has been sold, leased, and/or licensed to the general public; or,*

2. *has been offered for sale, lease, or license to the general public; or any item that evolved through advances in technology or performance and that is not yet available in the commercial marketplace, but will be available in the commercial marketplace in time to satisfy the delivery requirements under a Government solicitation."*

- Modified Commercial Item

  "*A modified commercial item is any item with modifications of a type customarily available in the commercial marketplace or minor modifications of a type not customarily available in the commercial marketplace made to meet Federal Government requirements. Such modifications are considered minor if the change does not significantly alter the nongovernment function or essential physical characteristics of an item or component, or change the purpose of the process.*"

- Ruggedized/Modified off the shelf: ROTS and MOTS

ROTS and MOTS are terms sometimes applied to components which are employed outside the manufacturers environmental specifications. These components have been "uprated" by the OEMs who employ extra testing and part screening to establish that components have extra margins that allow operation at higher temperatures, under radiation conditions, or other conditions which may be required for critical applications [4 and 6]. Note that these uprated components are not considered COTS by DoD.

While many definitions of COTS components exist in the industry, the DO-254 guidance is concerned with design assurance for safety requirements, irrespective of the components used. While the use of commercially available components will be shown to have several benefits, a significant challenge to the of use of COTS components lies in the fact that, by definition, the component is "developed by a supplier for multiple customers, whose design and configuration is controlled by the supplier's or an industry specification" (see glossary definition of COTS in reference 1).

1.2.2 Motivations to Employ COTS Components.

Three major benefits are sighted by reference 4 in using COTS components to meet defense needs.

1. Reduce overall cost of military hardware
2. Enhance defense supplier base
3. Maintain technological superiority by leveraging state-of-the-art technology rapidly

DoD R 5000.2R states that "Commercial and nondevelopmental items shall be considered as the primary source of supply" [5]. "The use of COTS products to build military systems accomplishes the following objectives:

- Reduces system acquisition costs by reducing development costs.

- Reduces the time required to field new military systems by reducing development time.

- Capitalizes on commercial research and development to field state-of-the-art systems more quickly.

- Offers opportunities to reduce life-cycle costs" [5].

Aviation safety may be enhanced by the use of state-of-the-art technology, at a practical cost through the use of COTS components, if the associated system safety requirements and aviation regulations can be met.

Reference 3 submits that the procurement strategy of the program may dictate the attractiveness of COTS components. Key factors include customer perception, COTS goals and preplanned product improvement, or technology insertion.

Examples of cost saving through the use of COTS or commercial components are prevalent in trade magazines such as reference 7, which reports:

- Lockheed Martin saved over $5 million per year by using low-cost commercial components on the Full Authority Digital Engine Control program.

- Lockheed Martin expects to save $10.3 million on the MK-1 Vertical Launching System through the use of commercial or COTS components.

- Lockheed Martin expects savings of $7.9 million through the use of plastic-encapsulated microcircuits instead of military-specified ceramic parts.

Reports such as these seldom describe the methods used to determine the cost savings. The military-specified components may cost 5 to 10 times more than commercial COTS components; however, the total cost of deploying COTS components includes a number of factors, not the least of which, is the cost of assurance that the part will function reliably in the intended environment.

1.2.3 COTS Market Trends.

A number of market trends are widening the gap between commercial market products and electronics required for critical systems. In the distant past, defense electronics development lead the industry; however, the volume of commercial production has grown to the point where military sales are less than 1% of the total worldwide market. Since the defense industry is now an insignificant portion of the market, other market forces are directing the commercial industry and are directing it in such a way that new challenges are being created for the critical component sector.

The mismatch between the military and commercial technology continues to widen. The semiconductor industry is currently moving from one generation of technology to the next at a rate of every 2 years, down from every 3 years [8] while product development cycles are down to a year or less [9].

It typically takes 10 years or more to develop or upgrade systems under the current DoD acquisition process. Defense systems are usually designed based on existing proven components and long delays occur between design and production. By the time the first production units are introduced into the field, the components used are not only technologically obsolete, but may no longer be generally available. Since these systems are expected to have long life times, 10 to 20 years or more, demand for maintenance parts will persist long after normal production has ceased [9]. This issue of microelectronics obsolescence is sometimes referred to as Diminishing Manufacturing Sources and Material Shortages (DMSMS) and is concisely described in reference 10.

The defense market differs significantly from the commercial market in that the commercial buyer tends to procure high volumes of a small number of devices, while defense buyers tend to procure a low volume of a large number of devices. One major semiconductor producer had 150 part numbers for the automotive market and 12,000 part numbers for the defense market [9].

Historically, fabrication facility costs have doubled with the introduction of each new generation of technology. Industry sources estimate the current cost of a state-of-the-art fabrication facility at over $1 billion. In order to profit with such large capital costs, the products must be targeted at markets which promise extremely high volumes and which have high turnover rates. State-of-the-art facilities are capable of 20,000 wafer starts per month. Production runs, for low-volume applications such as defense and safety critical systems, are not economically viable on these production lines [9].

As the complexity of the device increases, end-of-the-line or backside testing becomes more challenging and expensive. In some cases, it is already impossible to validate integrated circuits (IC) operation for every possible input condition. However, in large volume production, the process can be quality controlled to the point where some end-of-line testing becomes unnecessary. This level of quality is not attainable with low-volume production. Reference 9 observes "Standard parts, produced in millions, using statistical process controls, can have better quality than a part produced in batches of only a few thousand and then heavily (but partially) tested at the end of the line." Manufacture quality control is an important aspect of the Electronic Component Management Process for COTS components, which is identified in section 11.2 of reference 1, as the process which, combined with design assurance, forms the basis for the use of COTS components.

High-volume markets, such as the computer market, also tend to update or replace their equipment on a 3- to 5-year cycle in order to benefit from state-of-the-art performance. End-of-life wear-out is generally not seen in these markets which implies that the components may have large end-of-life reliability margins. Currently, ICs are designed for a 10-year life and a 1-year warranty. Since a 5-year life cycle may be more appropriate for this market, these commercial electronics may have "excessive end-of-life reliability." Market pressures may move commercial products to trade the perceived excessive end-of-life reliability for increased performance [8 and 11].

Integrated circuit producers continue to meet the expectations of Moore's law which predicts the performance/cost ratio of electronics to double every 18 months. Process improvements which increase yield have now reached such high levels that further improvement will not have significant impact. Scaling, i.e., the reduction of dimensions and/or voltages, is another technique used to reduce die size and thus produce more die per wafer. Scaling will be aggressively pursued to improve performance/cost ratios.

Scaling impacts of many areas are of interest to the critical systems designer. "One consequence of scaling (of dimensions and voltage) is that parts will become less robust" [8]. Scaled parts may have lower operating temperature margins which may preclude uprating or accelerated testing at elevated temperatures. The effectiveness of current test techniques may be degraded due to increases in leakage currents (see paragraph 3.10.2.3, Testing Methods, Iddq). Reduced charge per logic gate may increase susceptibility to single event upsets (SEUs) and reduce the device's radiation hardness relative to space, airborne, and land-based systems [8].

The rapid introduction of new materials technologies poses a new reliability risk. Historically, new material technologies were introduced one generation at a time. Up to 10 years may be required to fully understand the reliability implications of new materials. Currently, new materials are being introduced simultaneously for interconnects and dielectrics with the possibility of unknown reliability and new failure modes.

Aluminum interconnects are being replaced by copper to provide increased speed. While copper offers increased performance, copper is highly diffusive and may exhibit new failure modes. Diffusion barriers employed to limit diffusion cannot be increased to address the problem without reducing the performance gain. Volume production experience will be required to establish the reliability impact of this new technology [11].

Dellin's review of the Sematech Roadmap in reference 11 identifies the following top five areas requiring development as the industry moves to next generation technology:

- Reliability of Gate Dielectrics—direct tunneling; measuring and modeling
- Electromigration—building in reliability; standard test methods;
- Electrostatic Discharge—predictive models and methods; multivoltage ICs; testing
- Multilevel Metal/Dielectric Integrity—materials characterization; modeling; new dielectrics
- Hot Carrier–correlate tests with real ICs; models; simulation tools

Several sources for further information about trends in the semiconductor industry can be found in Section 8, Related Resources (see Semiconductor Industry Association (SIA) and Sematech web sites).

1.2.4 Consortium Research.

OEMs and component vendors concerned with high reliability electronics participate with and are supported by the work of a large number of consortiums, centers of excellence, and government agencies. Review of the membership of some of these organizations is instructive in identifying both the interested vendors and the dependant industries. Examples are the Center for Computer Aided Life Cycle Engineering (CALCE) at the University of Maryland, the Reliability Analysis Center (RAC), and the Electronics Quality/Reliability Center (EQRC) at Sandia. See section 8, Related Resources, for additional consortiums and web sites. See http://www.calce.umd.edu/general/membership/members/members.html for the complete list of CALCE members. A partial list follows in table 2.

TABLE 2. SELECTED CALCE MEMBERS

Organization	Organization
Boeing	Microsoft
Collins	Naval Surface Warfare Center
Delphi Delco Electronics	Nortel Networks
Ericsson Radio System	Philips
General Dynamics Information Systems	Raytheon Systems Company
General Motors (NAO)	Sandia National Labs
Honeywell	Schlumberger Oil Drilling Services
Jet Propulsion Lab.	Smiths Industries
Lockheed-Martin	Sun Microsystems
Lucas Aerospace	Visteon Automotive Systems

In summary, a number of market trends are causing the interests of the commercial market place to diverge from those of the critical electronics industry. These challenges must be adequately addressed when employing COTS components in critical systems and in compliance with the DO-254 guidance.

1.3 AREAS OF APPLICATION FOR SAFETY CRITICAL AND COTS COMPONENTS.

1.3.1 Characteristics of Safety Critical Applications.

- Safety critical systems, although used in several different industries, share important characteristics which are identified in the following paragraphs [12 and 13].

- The consequence of failure is high, usually resulting in the loss of life, large financial losses, compromise of national defense, or severe environmental damage. High reliability is required to reduce the risk of failure so components are subjected to extensive assurance methods and possibly stringent certification requirements.

- Low-volume consumer relative to major markets: component sources are dedicated to other markets or produce custom components for the low-volume market.

- Operation in harsh environments, including extreme temperature, humidity, shock and vibration, EMI, and radiation.

- Complex electronics, as previously discussed, where the behavior of the system may not be totally predictable by deterministic means. Application specific integration circuits (ASICs) are frequently utilized to provide the unique functionality required. Field Programmable Gate Arrays (FPGA) provide lower development costs and shorter design times.

1.3.2 Airborne Applications.

Airborne applications encompass all of the characteristics of the critical system to an extent found in no other industry.

- Highest consequence of failure, high reliability
- Extremely long life, significant parts obsolescence issues
- Extremely harsh environment
- Complex systems
- Regulation and certification
- Low volume, mainstream suppliers driven by other markets with diverging interests

Over half the development cost of both commercial and military aircraft is attributable to electronics [13].

Navigation, communication, and flight control systems contain significantly increased electronic content in both military and commercial aircraft. The OEMs, which supply the industry, are a diverse set of companies. Technology development will allow full function airborne systems to be applied to new applications, such as small aircraft, and will provide new capabilities which may enhance safety. "Features such as communications, navigation, and surveillance are becoming increasingly interdependent. Only competitors achieving integrated airborne systems will capture the future demand. Airlines are faced with demands to integrate benefits from many new technologies: free flight, air traffic management system (CNS/ATM), FANS, ATN, enhanced vision Global Positioning System (GPS), Satellite Communication (SATCOM), and data link are a few of the new concepts and technical improvements which are being promoted by aviation experts, civil aviation authorities, and avionics manufacturers" [13].

Current issues and concerns in commercial aviation are outlined in reference 14. The increased complexity of microelectronics hinders both functional simulation and device fault detection. Potential design errors are difficult to identify with existing tools, and these tools lack rigorous qualification in some cases. Device fault detection and verification is becoming a large part of device cost. Device complexity makes failure modes more difficult to identify and increases risk of latent faults.

"The most critical challenge facing the commercial avionics industry is in ensuring continuing affordable access to leading edge technology," according to reference 13. To meet this

challenge, new strategies, which incorporate affordable leading edge commercial components, need to be developed.

1.3.3 Applications in Other Industries.

1.3.3.1 Defense Electronics.

Reference 13 provides an excellent description of the defense electronics industry.

- Defense electronics are typically very complex systems.
- Defense spending on weapons procurement has dropped to half the amount spent 10 years ago.
- Mergers, acquisitions, and reorganizations have consolidated the OEM supplier industry to a handful of major players like Lockheed Martin, Boeing, and Raytheon.
- The life cycle of defense systems is significantly different than commercial industry and diverging.
- State-of-the-art technology being developed in the commercial sector can be of great value to the defense industry. Some examples include signal processing, computing power, display technology, and component miniaturization.

1.3.3.2 Nuclear Weapons.

Reference 15 provides a discussion of the role of critical ICs in the nuclear weapons industry and is summarized in the following paragraphs.

Although no ICs are currently used for safety critical functions, the reliability of ICs in use is 0.999 or higher over the 20-year life of the weapons. Several approaches to IC reliability are used. ICs meet Mil-spec qualifications and are tested at several temperatures and after burn-in. Operating temperature ranges from extreme cold to extreme hot. Destructive physical analysis and exhaustive failure analysis is performed. Wide design margins are used with component redundancy, where appropriate.

A field surveillance program is used, which does regular field sampling, with complete requalification, destructive physical analysis, and exhaustive failure analysis.

ICs incorporate built-in surety features such as canary fuses for metal migration and ring oscillators for hot carrier effects. Iddq testing is also used. Refer to section 3.10.2.3 for a description of Iddq testing.

A real-time parametric monitoring approach is under consideration for the future. Based on device defect mechanisms, the monitor would measure parameters, such as Iddq, in real-time and independent of system functionality and report system health and/or control surety outputs.

1.3.3.3 Space Industry.

Reference 16 reports "A wholesale move to off-the-shelf processors, system buses, and high-volume manufacturing disciplines is sweeping the satellite industry."

Lockheed Martin has developed a radiation-hardened version of the PowerPC 750 and is nearing completion of a radiation-hardened bridge chip for the CompactPCI bus.

Space Electronics Inc (SEI) has determined that the old Intel 486DX processors produced good radiation-tolerant specs and has procured as many as possible for certain satellite implementations.

Ground ranging stations are moving to off-the-shelf Pentek computer boards which incorporate the TMS 320 DSP processor.

Radiation-tolerant TMS320 processors and Actel 14100 FGPAs are being used in the next generation communication and intelligence satellite platform concept tests for a U.S. Air Force Research Lab experiment.

Electronics provided by Motorola, for 88 Iridium satellites, incorporated PowerPC 603 and 604 CPUs, almost exclusively surface mount technology, over 60 Ball Grid Array (BGA) devices.

1.3.3.4 Automotive Electronics.

Semiconductor usage in automotive electronics accounted for 3.3% of the market in 1995, compared to 0.8% for defense industries. This is considered low volume; however, the number of different parts the automotive industry buys is also low, as previously mentioned [13]. While automotive electronics is a small volume in worldwide sales, it is a market driver in the smaller, but significant, industry segment concerned with interface/driver components.

The automotive industry appears to rely on industry specifications to assure quality and reliability [17]. Rate of warrantee returns is the motivating quality factor. The supplier's manufacturing processes are audited for compliance with Automotive Electronic Council (AEC) specifications [17] such as:

- QS 9000 Quality systems requirements
- Q100 Parts capabilities
- Q001 Statistical methods for eliminating outliers (randomly defective parts)
- A100 Establishes a supplier's capability to provide parts of consistent production quality and reliability

1.3.3.5 Medical Electronics.

The global market for medical equipment can expect to experience significant growth of 10% to 20% over the next 10 years. Implantable defibrillators, pacemakers, diagnostic imaging systems,

and patient-monitoring equipment are important product areas. These products share the characteristics of critical systems, with the exception that most operate in benign environments [13].

The pacemaker device incorporates three ICs with reliability goals of less than ten unit failures in time (FITs) over 10 years. In this application, all U.S. failures are returned and a failure investigation is conducted. Sources suggest that some types of failures may go unreported, due to mitigation in the field, by doctors or technicians who reset or adjust the device.

Extensive testing is done at the die/wafer level. Minimum fault coverage of 95%-96% is maintained for "stuck-at", Iddq, and digital built-in self-test (BIST). The extensive die tests have demonstrated a 7× improvement in field failure rate. Improved wafer level testing and design for testability (DFT) are future areas of further improvement [18].

1.3.3.6 Other Industries.

References 19 and 20 document a survey of safety verification and validation methodologies for complex computer-based systems, which was carried out for the Federal Railroad Administration (FRA) in 1995. An in-depth summary of over 60 related documents is provided. Trends which were identified are reported in section 3.3.1 of this report.

Deep-well oil drilling, high-end computer systems, and robotics are other industries which share the need for critical electronics [13]. Little information was discovered in the nuclear industry.

1.3.4 Open System Application Trends.

In open system design, key interfaces are defined for the system under development. Physical modularity and functional partitioning are used to define subsystems/components. Efficient design will allow subsystems/components to be replaced or added without impacting other subsystem/components.

The open system approach is widely used in the commercial sector. It accommodates rapidly changing technology to provide performance upgrades and technology insertion. It promotes low cost, rapid development and supports multiple sources of supply. The light bulb is a simple, but elegant, example of an open system that allows performance upgrade, low-cost rapid technology insertion, and multiple sources of supply. The desktop computer is the most obvious example of an open system by virtue of the many modular subsystems it accommodates at several levels of interface—memory modules, video boards, communication boards, storage devices, video cameras, keyboards, joy sticks, etc.

The open system interface is defined by specification. Use of de facto specifications and widely accepted standards amplify the benefits of open system design. The interface standard is also a performance standard. Industry standards, such as the widely used Versa Module European (VME) bus standard, change over time, typically to enhance performance or add functionality. It is difficult to predict the success of emerging standards, such as CompactPCI, and many examples of short-lived standards can be identified. It is also a challenge to identify the proper

time to switch from one standard to another, as Apple recently did in switching from Small Computer System Interface (SCSI) to Universal Serial Bus (USB) for computer peripheral components. Many defense system providers are shifting from proprietary bus structures to open standard architectures in response to DoD directives and publicizing the shift as a move toward COTS.

An interesting trend toward open systems is currently emerging in System On a Chip (SOC) development. As the systems on the chip become more complex, the designs are incorporating intellectual property (IP) from multiple sources, and a need for open system's standardization is emerging to allow IP from different vendors to be properly interfaced and verified. The Virtual Socket Interface (VSI) Alliance [21] is currently developing interface standards for IP modules and coping with the wide variety of challenges posed by the task, including testing strategies.

Successful adoption of the open system approach will require new approaches to test objectives, philosophy, and criteria [22]. The test approach must focus on functional performance and "form, fit, function, and interface (F^3I)" to allow subsystems/components within the system to be changed during development, fielding, and life-cycle support. The designers of such open systems will not focus on the development of new components, but rather the integration of existing subsystem/components. Some question if this approach will result in a long-term decline of technical innovation, while others see it as a way to benefit from rapid technology insertion. This radically different approach is being evaluated in several DoD demonstration programs—the Army Intelligence and Electronic Warfare Common Sensor (IEWCS); the Navy's New Attack Submarine (NSSN), F-15, F/A-18, and AV-8B common processor pilot programs; and the Seventh Fleet Command Ship (USS Blue Ridge) [22].

Open systems share all the challenges associated with COTS component usage. The commercial industry controls the development of the component and controls the functional content of the component. Life-cycle support of open architecture-based systems must address a difficult set of issues, which includes assurances for performance, reliability, and compliance with interface standards, as well as configuration management and change control. The open system approach will require novel design and test techniques to meet the assurances needed for safety critical functions.

1.4 TYPES OF COMPONENTS IN USE.

1.4.1 System/Subsystem Components.

> *"The radar and sensors, communication and navigation systems, data processing equipment, and integrated avionics systems, are built by a diverse set of companies (e.g., Hughes Electronics, Electronic Sensors and Systems Division of Northrop Grumman, Litton Industries, Rockwell Collins, TRW, International Ericsson of Sweden, Daimler-Benz Aerospace AG Sensor Systems of Germany, GEC-Marconi Sensors of United Kingdom, and Dassault Electronique of France)"* [13].

The web sites for a number companies were reviewed. The hyperlinks within this document were current at the time of publication; however, they may or may not function at later dates. While innumerable products are represented, the information relative to commercial airborne systems was found to be sparse of description relative to the use of COTS components. For example:

- Lockheed Martin Commercial Full Authority Digital Engine Controls (FADECs) incorporate custom-designed integrated circuits and 32 bit 68020 microprocessors http://www.lmcontrolsystems.com/FactSheets/commlFADEC.pdf

- Boeing Electronics Products provides avionics for the entire family of commercial jetliners which include 777 avionics, 777 Warning Electronics Units, Cabin management systems. The web site does not indicate if COTS components are employed. http://www.boeing.com/defense-space/infoelect/electprod/

- Litton's GPS sensor is described at http://www.littonapd.com/html/ltn-2001.html. The LTN-2001 is certified on a number of Boeing and Airbus aircraft and may be an example of a COTS component which would be procured as a "certifiable" device. Litton claims their "AIME™ technology,....solves GPS integrity problems and provides a means of achieving sole means of navigation with GPS accuracy for commercial aircraft."

While COTS components may well be used and provide benefits, apparently these companies do not consider the use of COTS components to be a market discriminator in and of itself.

Use of COTS components was more frequently mentioned for military products, perhaps due to the military's emphasis on COTS procurements. While not directly applicable to commercial airborne systems at this time, the military programs may be fostering the development of COTS components, which will transition to the commercial aviation sector in the future. Open architectures, VME back planes, and microprocessors were most frequently mentioned with respect to COTS usage.

> *"Command-and-control programs that rely heavily on data and voice communications are providing an early test of the Defense Department's commercial off-the-shelf (COTS) acquisition strategy." Lockheed Martin (LM) is thought, by some, "to control two-thirds of all contracts in the military command, control, and intelligence programs"* [23].

The USAF/Boeing C-17 Globemaster III incorporates two Core Integrated Processors (CIP), which provides central control of all of the aircraft avionics systems. According to LM, the CIP "leverages flight-proven "off-the-shelf" designs for hardware and software." The CIP uses VME back-plane communication between modules and incorporates the MIPS R4400 processor, which provides "off-the-shelf multisource availability." http://www.lmcontrolsystems.com/FactSheets/c-17%20cip.pdf

LM provides the flight control electronics set for the F/A-18. It is a quadraplex digital system incorporating "microprogrammable digital processors specifically developed for flight control

applications." Note that this is specifically not COTS hardware. http://www. lmcontrolsystems. com/FactSheets/f-18.pdf

LM provides Flight Control Electronics Assembly-Upgraded (FCEA-U) system for the JAS 39 Gripen multimission aircraft. The digital, full authority fly-by-wire control is triplex redundant and incorporates processors by Motorola (68040) and Texas Instruments (TMS 320C30). http://www.lmcontrolsystems.com/FactSheets/jas-39.pdf

The Raytheon Command, Control, Communication, and Information systems are using COTS technologies, open systems architectures, and VME standards-based designs to produce lighter, smaller systems with expanded capabilities at reduced cost. Over the last 10 years, the COTS content of Raytheon workstations has increased from 15% to 95%. http://www. raytheon.com/c3i/ c3iproducts/c3i046/c3i046.htm

General Dynamics Information Systems Open System Mission Computer (OSMC), used on AV-8B, uses a common processor module (board) provided by DY 4 Systems, based on PowerPC 603e. The VME bus standard is used on the OSMC. http://www.gd-is.com/products/ process/osmc1.html

The following web sites were also reviewed. While these companies may make use of COTS components, no definitive information was discovered.

- Teledyne Controls Aircraft Systems: http://www.teledyne-controls.com/air_sys.html
- BFGoodrich Avionics Systems: http://www.bfgavionics.com/docs/products.html
- Rockwell Collins: http://www.collins.rockwell.com/at-systems/products/
- TRW Space & Electronics Group: http://www.trw.com/seg/avionics.html
- Harris: http://www.govcomm.harris.com/airborne/
- Northrop Grumman: http://sensor.northgrum.com/, http://www.northgrum.com/ isa_www/bus_areas/index.htm
- Smiths Industries: http://www.smithsind-aerospace.com/
- Kaiser Electronics: http://www.kaiseraerospace.com/pages_00q1/01_ak.html
- Woodward: http://www.woodward.com/AES/news/lockheed.cfm
- Hughes: http://www.hughes.com/
- Thiokol Propulsion: http://www.thiokol.com/Index.htm

1.4.2 Board/Module Components.

Commercial computer board sales continue to increase. Projections by Venture Development Corporation [24] indicate the dollar value of boards shipped in 2002 will be nearly double that of 1994. By 2004, the value may be double that of 1999, indicating a rapid move to adoption of third-party computer boards in new designs. The increase in board sales may also be an indication of the commercial trend toward "open systems" architectures in large systems.

For the most part, these boards are designed to comply with a bus interface. Reference 24 survey data seems to indicate a trend away from proprietary bus structures towards those supported by an industry standard. VME is probably the most popular bus for military/defense systems. The PCI bus, made popular in desktop computing, has rapidly increased in popularity in the communications industry, in part because of the "hot swap" capability it provides. PCI is presenting a formidable challenge to VME for communications systems, however, VME standards continue to evolve to address the need for increased bandwidth.

A survey of the 20 most frequently mentioned board manufacturers, (see reference 24) shows a few manufacturers consistently mentioned in the top few positions. Manufacturers who support the ruggedized market are well represented in the survey data. Ruggedized designs initially targeted at severe environment DoD applications may be gaining a foothold in the less-severe industrial market.

The commercial telecommunications market is perceived as a large new opportunity for open system board manufacturers. In fact, for some manufacturers, COTS may stand for "Concentrate On Telecommunications Sales." These large commercial systems are easily partitioned and based on industry standard back-plane busses such as VME and CompactPCI. Modularity allows spare capacity and rapid replacement of failed boards, in some cases without having to power down the system. While much excitement has been generated in the trade media, the market has been slow to takeoff.

Data and voice communications are also key functionality for DoD command and control programs, which are moving towards open system architecture. Several demonstration programs are underway, with initial successes reported. The DoD Open Systems Core Avionics Requirement (OSCAR) program upgraded a Harrier AV-8B with a VME bus based system which incorporated computer boards provided by a commercial board manufacturer. The DY 4 computer board includes a 200-MHz PowerPC 603e microprocessor [25].

Reference 26 observes that military (and critical airborne) systems development processes require COTS vendors to provide services that are beyond those normally required by the commercial sector. "To meet this class of customer's program needs, the COTS provider must provide:

- A leading-edge technology solution that meets the program's requirements
- A product with a low-risk path to future technology insertions
- A product that is guaranteed across extended environmental specifications
- The capability to guarantee a rigorous class of program and product management

- The ability to deploy the solution in a custom form-factor.

Note: to meet the second through fifth requirements, the COTS Digital Signal Processor (DSP) provider must make a definite commitment and investment."

Major commercial board vendors seem to approach the ruggedized market in two ways: directly and indirectly through third-party value-added vendors. The direct approach vendors provide boards which are typically conduction cooled and specified for operation over extreme ranges of temperature and shock/vibration. Typically, several ranges of ruggedization are offered, ranging from commercial to severe [27, 28, and 29]. Third-party vendors provide boards specified for operation in severe environments based on products designed and produced by major commercial manufacturers. The major vendor product is specified over commercial operating ranges, however, the same design accommodates ruggedized versions which are provided to OEMs through third-party, value-added vendors [30].

1.4.3 Microelectronics Components.

1.4.3.1 Commercial Microelectronics.

The QML 38535 rev 012 lists 28 IC manufacturers which have chosen to continue support of the "mil-spec" IC market. (See section 3.3.2, Standards, for discussion of the role of QML and list of QML vendors.) Intel and Motorola are major commercial suppliers missing from the list. Intel dropped its military specification products in 1997. At that time, Intel supplied approximately 8% of the $1.4 billion market for military ICs [31]. Motorola has formed alliances with third-party vendors, like Thomson CSF, to provide extended operating range versions of the Motorola commercial products like the PowerPC 603e [30].

Cypress semiconductor is an example of a QML supplier that supports the Standard Microcircuit Drawing (SMD) program as well as MIL-STD-883 and MIL-PRF-38535. Cypress is also certified for compliance with the following industrial standards: ISO 9001, ISO 9002, and ISO 14001. Cypress products include FIFOs, PROMs, SRAMs, Clock Buffers, Bus Logic, PLDs, and VME bus products. Cypress lists among its customers Lockheed Martin Information Systems Company, United Technologies Hamilton Standard, Raytheon Electronic Systems, Raytheon Missile System Division, and GE Aerospace [32].

Actel and Xilinx are both QML suppliers of FPGAs. The FPGA is a popular component for avionics design because it allows complex logic to be incorporated in a high-density package with short development time relative to a custom ASIC. FGPAs incorporate 14,000 equivalent gates, and future devices will provide up to 40,000 gates. While Actel's FPGA approach uses one-time programmable technology, "special test modes allow functional testing of the unprogrammed devices at essentially 100 percent fault coverage" [33]. Xilinx is teaming with Los Alamos National Laboratory to evaluate the sensitivity of Xilinx Virtes reprogrammable FGPAs to Single Event Upset (SEU) events caused by cosmic rays. The FPGAs will be used to design data processors for space-based remote-sensing applications [34].

National Semiconductor is an example of a supplier who provides a number of COTS ICs which are targeted at the avionics industry for use in flight controls data buses, auto pilot flight director

computer, actuator surface control, air data inertia reference units, and control and display units among other systems [35].

Rochester Electronics is an example of an after-market supplier who claims to be the world's largest supplier of discontinued semiconductors. Third-party suppliers such as Rochester are franchised by leading semiconductor manufacturers to continue manufacturing parts discontinued by the original manufacturer [36].

1.4.3.2 Application Specific Integrated Circuits (ASICs).

Honeywell Commercial Avionics is an example of an ASIC supplier whose services are tailored to the avionics industry. They claim to support any volume, long life cycles, and -55° to 125°C temperature ratings. Mixed signal, i.e., both analog and digital, designs can be incorporated into System On a Chip (SOC) solutions [37]. There are two categories of ASIC: the standard cell and the gate array.

In the standard cell, the mask is user defined. The functions incorporated in the standard cell ASIC can be totally customized and are typically partitioned into blocks or cells. The function cells may be newly designed or may incorporate previously designed circuitry for both analog and digital functions. Cell functions include RAM, ROM, random logic, state machine logic, CPUs, DSPs, and analog functions such as voltage regulators and A/D converters. In the design, the cell placement and interconnects are optimized for minimum number and length, which results in fewer layout-induced problems and small die area.

Gate arrays consist of a large array of identical logic blocks which are typically prefabricated. Only the interconnection of the logic blocks is customized by the user. In the mask programmable version, the interconnect layer is fixed by the custom mask. Field Programmable Gate Arrays (FPGAs) incorporate additional logic to program a matrix of interconnects between the logic blocks. The interconnection matrix may pose a bottleneck in the design, prompting the designer to move to a larger FPGA IC.

Global sales of standard cell ASICs seem to be two to three times that of mask programmable gate arrays and show growth for standard cell and decline for gate arrays. The complexity of the standard cell ASIC is increasing towards SOC, and will require more integration of the customer-owned design tools as well as use of third-party functional intellectual property (IP) in cells of the ASIC [38].

Vendors are offering specialized ASICs which incorporate core functions such as PCI interfaces in standard cell, plus 120K gates of FPGA. These chips are obviously targeted at the high-volume commercial computer industry, but are indicative of future trends. FPGAs are now available with 400K gates and 672 input/output (I/O) pins [39].

SOCs will dominate the IC market in 5 to 7 years, accounting for over half of the total IC business. While the dollar volume will increase from $3 billion in 1998 to $21 billion in 2002. At the same time, the design cycle time will reduce from 10 months in 1998 to less than 6 months as designers increase the complexity of the SOC at an exponential rate [40].

2. KEY COMPONENT ATTRIBUTES DERIVED FROM DO-254 OBJECTIVES AND GUIDANCE.

The purpose of this section is to review the DO-254 objectives and guidance in order to identify attributes, which are required of a component, to successfully meet DO-254 objectives. Selected sections of the guidance are presented that are pertinent to components in general, and COTS components in particular. DO-254 quotes are shown in italics. Sections of the guidance which are the source of specific attributes have been underlined in the guidance text to aid in identification. Grouping of the attributes, as described in the Key Attributes Summary, results in the following key attributes:

Design Assurance	Service Experience
Component Reliability	Configuration Management
Standards	Production Practices
Failure Modes	Verification Testing
Operation Beyond Mfg. Spec.	Role of COTS Tools in Design and Verification
Upsets	

2.1 COTS COMPONENT USAGE AND PROCUREMENT.

"COTS components are used extensively in hardware designs, and typically, the COTS components design data is not available for review. The certification process does not specifically address individual components, modules, or subassemblies, as these are covered as part of the specific aircraft function being certified. As such, the use of COTS components will be verified through the overall design process, including the supporting processes, as defined in this document. The use of an electronic component management process, in conjunction with the design process, provides the basis for COTS components usage" (see section 11.2 of reference 1).

"COTS component procurement guidance is not the intent of this document, but feedback of procurement issues should be managed and resolved by the applicant when they have significant impacts on hardware design assurance.

Major concerns include:

1. *Actual availability of COTS component design assurance data as required by this document.*

2. *Variations in component parameters that depend on production batches may not be identified, even by robustness tests.*

3. *Evolving aspects of electronic component technology.*

4. *COTS components which become nonprocurable"* (see section 11.2.2 of reference 1).

Attributes: Component design assurance data, production control of parameter variation, procurable component, and stable technology

2.2 HARDWARE SAFETY ASSESSMENT (HSA).

Objectives:

> *"Given the safety, functional and performance requirements allocated to the hardware by the system process, the hardware safety assessment determines the hardware design assurance level for each function and contributes to determining the appropriate design assurance strategies to be used"* (see section 2.3 of reference 1).

2.2.1 Hardware Safety Assessment and Hardware Design Assurance Level.

The HSA receives, as input from the System Safety Assessment (SSA), the safety requirements associated with the functions allocated to the hardware. The allocated function is assigned a system development assurance level by the SSA System Process. The HSA process then determines the Hardware Design Assurance Level, for the hardware used to implement the function, by assessing if any *"failure or anomalous behavior"* of the hardware used to implement the function will cause a failure of the associated system safety function. If this proves to be the case, then the hardware function is assigned the Hardware Design Assurance Level associated with the designated System Development Assurance Level. Levels of criticality are fully described in Table 2-1 of reference 1 and designated as follows:

Hardware Design Assurance Level Designations

Level A	Catastrophic
Level B	Hazardous/Severe-Major
Level C	Major
Level D	Minor
Level E	No effect

DO-254 notes that there are two types of anomalous behavior of the hardware which are assessed using various qualitative and quantitative assessment methods.

The first type of anomalous behavior, random faults, may be assessed through quantitative means, including *"Statistical failure assessment and prediction methods, which are based on hardware failure rates, redundancy, separation and isolation, failure mode statistics, probability analysis, component de-rating, stress analysis, and manufacturing process control"* (see section 2.3.2 of reference 1).

The second type of anomalous behavior includes design errors in a hardware item and upsets to the hardware. *"Unlike random failures of hardware, neither design errors nor some types of upsets are statistically predictable, and both may cross redundancy boundaries in the form of common mode faults. Redundancy management techniques and quantitative assessment methods to be used should be selected so that potential common mode faults and the effects of upsets are*

precluded or mitigated when necessary. Although difficult to assess quantitatively, safety risk from design errors and upsets can be effectively assessed by a practical application of qualitative safety assessment methods. Analysis techniques, such as fault tree analysis, common mode analysis, and functional failure modes and effects analysis (F-FMEA), are fundamentally qualitative methods, and can be used to address hardware design errors and upsets" (see section 2.33 of reference 1).

Attributes: Identifiable failure modes, failure rate data, component rating data, component response to upsets, and manufacturing process control

2.2.2 Design Assurance Strategy.

The design assurance strategy is determined by the criticality level assigned to the hardware function and by the complexity of the hardware components follows:

- Levels D and E: simply document the design assurance approach
- Level C: document fail-safe aspects and document the design assurance approach
- Levels A or B with simple hardware: same as level C
- Levels A or B with complex hardware: develop a design assurance strategy plus same as level C

> *"For a simple hardware item, extensive documentation of the design process is unnecessary. The supporting processes of verification and configuration management need to be performed"* (see section 1.6 of reference 1).

Appendix B of DO-254 provides guidance for the development of a design assurance strategy for level A or B, using Functional Failure Path Analysis (FFPA), and describes specific methods of design assurance.

> *"For each level A and level B function, determine the means of implementing the function or the subfunctions and analyze the design assurance options. The assurance data available or expected to be available for the implementation of the function or subfunction should be complete and acceptable for the design assurance strategy or strategies chosen. If the assurance data available or expected to be available is complete, correct and acceptable, then no further decomposition is necessary"* (see appendix B section 2.1 of reference 1).

> *"This assessment process is iterative. If there is no acceptable method of design assurance for a FFP, the decomposition and evaluation process is repeated or the architecture or implementation of the hardware function changed until an acceptable method of design assurance has been determined and acceptable assurance data is provided or can be provided for each level A and level B FFP"* (see appendix B section 2.1 of reference 1).

Attributes: Acceptable Design Assurance data for complex level A or B

2.2.3 Design Assurance Methods.

Design Assurance methods for level A or B functions include architectural design features, product service experience, and *application of advanced verification methods, such as Elemental Analysis, Formal Methods, Safety-Specific Verification Analysis, or other applicant-proposed and certification authority-accepted methods"* (see appendix B section 3.3 of reference 1).

2.2.3.1 Architectural Design Features.

"Architectural design features, such as dissimilar implementation, redundancy, monitors, isolation, partitioning, and command/authority limits, can be specifically employed to mitigate or contain the adverse effects of hardware design and implementation errors" (see appendix B section 3.1 of reference 1).

2.2.3.2 Product Service Experience.

> Product *"Service experience may be used to substantiate design assurance for previously developed hardware and for COTS components. Service experience relates to data collected from any previous or current usage of the component. Data from non-airborne applications is not excluded.*
>
> *Note: Wide and successful use of an item in service may provide confidence that the item's design is mature and free of errors and that the manufacturing quality of the item is demonstrated"* (see section 11.3 of reference 1).
>
> *"Section 11.3 provides basic guidance on how to assess product service experience data for applicability for use in airborne hardware. For Level A and B functions that use previously developed hardware as part of the design, additional design assurance is necessary. This assurance can be provided in the following manner"* (see section 3.2 of reference 1).

2.2.3.3 Elemental Analysis.

Elemental analysis extends the FFPA to a level of decomposition where each functional element within the complex hardware can be acceptably verified. This method could be used for ASICs or Programmable Logic Devises (PLDs) where detailed design data is available and under configuration control. Unused functions which may be present *"should either be shown to be isolated from the other used functions or shown to present no potential anomalous behavior that could have an adverse effect on safety"* (see appendix B section 3.3.1.2 of reference 1).

2.2.3.4 Safety-Specific Analysis.

> *"Safety-specific analysis is based on the concept that a potentially latent design error can affect a hardware item's output only when specific input stimuli expose it. Therefore, to properly stimulate and expose the safety errors of concern, the*

subset of input cases for which safe operation is necessary is identified, and then appropriate equivalence classes from that subset are included in the verification tests. During execution of these test cases, the item's outputs are evaluated for absence of specific anomalous behaviors that could result in unsafe output conditions. The safety-specific analysis is used to bound the set of input conditions to be applied in the verification test cases so that a potentially infinite set of input test cases do not have to be addressed."

"Note: The implementation may also bound the input set and conditions so that it is not possible or is adequately improbable that the implementation would allow an input outside the limits tested."

"The safety-specific analysis method is equally applicable to either COTS hardware or custom circuits and components because it is able to use user guide data about those circuit and components instead of detailed internal design data. By combining the user guide data with this more detailed application of the FFPA method, the safety-specific analysis is able to successfully determine the safety-sensitive aspects of circuit and component usage and the associated internal FFPs where design error removal emphasis is needed" (see appendix B section 3.3.2 of reference 1).

2.2.3.5 Formal Methods.

Formal methods may be employed to gain design assurance. *"The level of design assurance depends upon the fidelity of the models employed"* (see appendix B section 3.3.2 of reference 1). *"Tools used should be assessed and, if necessary, qualified as described in section 11.4"* (see appendix B section 3.3.3 of reference 1).

Attributes: acceptable product service experience, detailed design data, appropriate design models for Formal Methods, and assessed tools for formal methods

2.3 HARDWARE PLANNING PROCESS.

Objectives:

"The purpose of the hardware planning process is to define the means by which the functional and airworthiness requirements are converted into a hardware item with an acceptable amount of evidence of assurance that the item will safely perform its intended functions.

The objectives of the hardware planning process are:

1. *The hardware design life cycle processes are defined.*

2. *Standards are selected and defined.*

3. *The hardware development and verification environments are selected or defined.*

4. *The means of compliance of the hardware design assurance objectives, including strategies identified using guidance in Section 2.3.4, are proposed to the certification authority"* (see section 4.1 of reference 1).

Attributes: Standards, assessed development tools, and assessed verification tools

2.4 HARDWARE DESIGN PROCESS (HDP)—REQUIREMENTS CAPTURE AND CONCEPTUAL DESIGN OBJECTIVES.

2.4.1 Hardware Design Process—Requirements Capture Objectives.

1. *"Requirements are identified, defined and documented. This includes allocated requirements from the PSSA and derived requirements from the hardware safety assessment.*

2. *Derived requirements produced are fed back to the appropriate process.*

3. *Requirement omissions and errors are provided to the appropriate process for resolution."* (see section 5.1.1 of reference 1).

"Note: Derived requirements may address conditions, such as:

A. *Specific constraints to ensure that functions of a higher design assurance level can withstand anomalies of functions of a lower design assurance level as seen at the interface of the function with the lower design assurance level*

B. *The range of data inputs considering typical and full-scale data values as well as the high and low states of bits in data words or control registers.*

C. *Power-up reset or other reset states.*

D. *Supply voltage and current demands.*

E. *Performance of time-related functions, such as filters, integrators and delays.*

F. *State machine transitions that are possible, whether they are anticipated or not.*

G. *Signal timing relationships or electrical conditions under normal and worst-case conditions.*

H. *Signal noise and cross-talk.*

I. *Signal glitches in asynchronous logic circuits.*

J. *Specific constraints to control unused functions"* (see section 5.1.2 of reference 1).

Attributes: Identifiable anomalous behavior, identifiable unused functions

2.4.2 Hardware Design Process Conceptual—Design Objectives.

"1. *The hardware item conceptual design is developed consistent with its requirements.*

2. *Derived requirements produced are fed back to the requirements capture or other appropriate processes.*

3. *Requirement omissions and errors are provided to the appropriate processes for resolution."* (see section 5.2.1 of reference 1).

Attributes: none

2.5 HARDWARE DESIGN PROCESS—DETAILED DESIGN PROCESS OBJECTIVES.

"1. *The detailed design is developed from the hardware item requirements and conceptual design data.*

2. *Derived requirements are fed back to the conceptual design process or other appropriate processes.*

3. *Requirement omissions or errors are provided to the appropriate processes for resolution"* (see section 5.3.1 of reference 1).

"The detailed design data describes the data necessary to implement the hardware item consistently with its requirements. Depending on the hierarchical level of the hardware item, this may include top-level drawing, assembly drawings, interconnection data, parts data, HDL hardware description, reliability data, test methodology data, list of unused functions in selected components and actions taken to assure they will not compromise the safety of the hardware item, installation control data, and hardware/software interface data" (see section 10.3.2.2 of reference 1).

Attributes: Reliability data, test methodology data, list of unused functions

2.6 HARDWARE DESIGN PROCESS—IMPLEMENTATION PROCESS OBJECTIVES.

"1. *A hardware item is produced which implements the hardware detailed design using representative manufacturing processes.*

2. *The hardware item implementation, assembly and installation data is complete.*

3. *Derived requirements are fed back to the detailed design process or other appropriate processes.*

4. *Requirement omissions and errors are provided to the appropriate processes for resolution"* (see section 5.4.1 of reference 1).

Attributes: Implementation, assembly and installation data

2.7 HARDWARE DESIGN PROCESS—PRODUCTION TRANSITION OBJECTIVES.

"1. A baseline is established that includes all design and manufacturing data needed to support the consistent replication of the hardware item.

2. *Manufacturing requirements related to safety are identified and documented and manufacturing controls are established.*

3. *Derived requirements are fed back to the implementation process or other appropriate processes.*

4. *Errors and omissions are provided to the appropriate processes for resolution"* (see section 5.5.1 of reference 1).

Attributes: manufacturing controls

2.8 VALIDATION PROCESS OBJECTIVES.

"1. Derived hardware requirements against which the hardware item is to be verified are correct and complete.

2. *Derived requirements are evaluated for impact on safety.*

3. *Omissions and errors are fed back to the appropriate processes for resolution"* (see section 6.1.1 of reference 1).

Attributes: none

2.9 VERIFICATION PROCESS OBJECTIVES.

"1. Evidence is provided that the hardware implementation meets the requirements.

2. *traceability is established between hardware requirements, the implementation, and the verification procedures and results.*

3. *Acceptance test criteria are identified, can be implemented and are consistent with the hardware design assurance levels of the hardware functions.*

4. *Omissions and errors are fed back to the appropriate processes for resolution"* (See section 6.2.1 of reference 1).

"Verification process objectives may be satisfied through a combination of methods, such as reviews, analyses, and the development and execution of tests" (see section 6.2.2 of reference 1).

"A review is a qualitative method for evaluation of the plans, requirements, design data, design concept or design implementation" (see section 6.3.3 of reference 1).

"Analysis is a detailed, repeatable, analytical method for evaluation of specific hardware item characteristics to demonstrate that a specific requirement is met.

Analyses may include a detailed examination of the functionality, performance, traceability and safety implications of a hardware item function and its relationship to other functions within the airborne system or equipment. Analysis alone or in combination with other verification methods provides evidence that a requirement is correctly implemented. Analysis should be based on data provided by the design process, service experience or other available databases.

Simulation is an important design analysis tool both for visualization of circuit operation and for higher level functional operation. Simulation can be used to analyze the impact of production variations in hardware parameters that would be difficult to do using other verification means and thus build confidence in reduction of design errors affecting safety due to these variations. Since the results depend on the models and scenarios employed, simulation results alone cannot be used for the purpose of certification credit without supporting evidence of their validity" (see section 6.3.2 of reference 1).

"Examples of analysis include:

1. *Thermal Analysis. Thermal analysis verifies that the design implementation meets the requirements when exposed to the operating thermal environment.*

2. *Stress Analysis. Stress analysis verifies that components meet de-rating criteria over the required operating range.*

3. *Reliability Analysis. Reliability analysis establishes whether the design implementation satisfies the reliability requirements of the product.*

4. *Design Margin Analysis. Design margin analysis verifies that the design implementation satisfies its functional requirements given the variability of components.*

5. *Similarity Analysis. Similarity analysis compares characteristics and usage to those of systems previously certified.*

6. *Simulation Analysis. A simulation analysis compares the simulation results and expected results"* (see section 6.3.2 of reference 1).

"Testing performed for certification credit requires a configured item." "When it is not feasible to verify specific requirements by exercising the hardware item in its intended operational environment, other verification means should be provided, and justified." "Each requirement to be validated or verified by test should be identified.

Environmental qualification test requirements are part of these requirements" (see section 6.3.1 of reference 1).

Attributes: Configured item, design process data, service experience data, production variations in hardware parameters, operational environment, environmental qualification, and evidence that the component meets the requirements

2.10 CONFIGURATION MANAGEMENT PROCESS OBJECTIVES.

"1. Configuration items are uniquely identified and documented.

2. *Consistent and accurate replication of configuration items is ensured.*

3. *A controlled method of identifying and tracking modification to configuration items is provided"* (see section 7.1 of reference 1).

"Note: The detail to which components, such as ASICs, configured PLDs, printed circuit boards, and black boxes are identified, is determined by the Configuration Management Plan.

Configuration identification should be established for COTS components and previously developed hardware items before they are used in a baseline" (see section 7.2.1 of reference 1).

"The purpose of the change control activity is to ensure the recording, evaluation, resolution, and approval of changes. Change control should be implemented in compliance with the configuration management plan and should be started no later than the establishment of the baseline from which certification credit is to be obtained.

Guidance includes:

1. *Change control should preserve the integrity of the configuration items by providing protection against unauthorized change.*

2. *Change control should ensure that a change is assessed to determine whether or not the configuration identity needs to be updated.*

3. *Changes to configuration items under change control should be recorded, approved, and tracked. Approval authority is defined in the configuration management plan.*

Note 1: Problem reporting is related to change control, since resolution of a reported problem may result in changes to configuration items.

Note 2: It is generally recognized that early implementation of change control assists the control and management of process activities.

4. *Change control should ensure traceability of changes to the reason for the change.*

5. *Change control should ensure that the impact of the change is assessed to determine the effect of the change on the outputs of the processes and that the output data is updated.*

Note 1: Some or all of the activities of the processes may need to be repeated from the point at which their outputs are affected.

Note 2: It should be recognized that a change to the manufacturing tools, technology processes or external components may impact the design" (see section 7.2.4 of reference 1).

"The configuration management process for the new application of previously developed hardware should include, in addition to the guidance of Section 7:

1. *Traceability from the hardware product and life cycle data of the previous application to the new application.*

2. *Change control processes that can manage change requests from different applications of the common item"* (see section 11.1.5 of reference 1).

Attributes: Process control, process change control, process change reporting

2.11 PROCESS ASSURANCE OBJECTIVES AND CERTIFICATION LIAISON PROCESS OBJECTIVES.

Process assurance objectives

> *"1. Life cycle processes comply with the approved plans.*
>
> *2. Hardware design life cycle data produced complies with the approved plans.*
>
> *3. The hardware item used for conformance assessment is built to comply with the associated life cycle data"* (see section 8.0 of reference 1).

Certification liaison process objectives

> *"The purpose of the certification liaison process is to establish communication and understanding between the applicant and the certification authority throughout the hardware design life cycle to assist in the certification process"* (see section 9.0 of reference 1).

Attributes: none

2.12 STANDARDS.

DO-254 provides guidance relative to use of standards in the hardware design life cycle; however, it does not specify particular standards. The adoption of standards seems to be left to the applicant.

> *"Hardware design standards are used during the conceptual design process and detailed design process, and may define the rules, procedures, methods, guidelines and criteria for developing and specifying the hardware design.*
>
> *Hardware design standards may include:*
> *...Guidelines on design methods.*
> *Guidelines on the use of hardware design tools.*
> *Guidelines for electronic component selection.*
> *Guidelines for assessing design alternatives.*
> *Guidelines for assessing the fail-safe and fault-tolerance design constructs...."* (see section 10.2.2 of reference 1).

Attributes: Appropriate application of standards

2.13 ELECTRONIC COMPONENT MANAGEMENT PROCESS.

> *"The use of an electronic component management process, in conjunction with the design process, provides the basis for COTS components usage"* (see section 11.2 of reference 1).

"Electronic component management for COTS components is an important supporting process associated with the design and development of hardware. The processes of electronic component management apply to COTS electronic components. While there are both business and technical aspects of this process, this section only deals with the technical aspects as they impact certification.

"Certification credit may be gained by establishing that:

1. *The component manufacturer can demonstrate a track record for production of high quality components.*

2. *Quality control procedures are established at the component manufacturer.*

3. *There is service experience supporting the successful operation of the component.*

4. *The component has been qualified by the manufacturer or by means of additional testing, which establish the component reliability.*

5. *The component manufacturer has control of the component quality level or that this is assured by means of additional component testing.*

6. *The components have been selected on the basis of technical suitability of the intended application, such as component temperature range, power or voltage rating, or that additional testing or other means has been used to establish these.*

7. *The component performance and reliability are monitored on a continuous basis, with feedback to component manufacturers concerning areas that need improvement"* (see section 11.2.1 of reference 1).

Attributes: Quality control, component technical suitability, component reliability, and service experience

2.14 TOOL ASSESSMENT AND QUALIFICATION.

"Tools, both hardware and software, will normally be used during hardware design and verification. When design tools are used to generate the hardware item or the hardware design, an error in the tool could introduce an error in the hardware item. When verification tools are used to verify the hardware item, an error in the tool may cause the tool to fail to detect an error in the hardware item or hardware design. Prior to the use of a tool, a tool assessment should be performed. The results of this assessment and, if necessary, tool qualification should be recorded and maintained.

The purpose of tool assessment and qualification is to ensure that the tool is capable of performing the particular design or verification activity to an acceptable level of confidence for which the tool will be used" (see section 11.4.1 of reference 1).

Attributes: Employ qualified design tools, employ qualified verification tools

2.15 DO-254 APPENDIX A—MODULATION OF HARDWARE LIFE CYCLE DATA BASED ON HARDWARE DESIGN ASSURANCE LEVEL.

"This appendix provides guidance for the modulation of the hardware design life cycle data based on the hardware design assurance level. It also provides guidance concerning the requirements for independence during the verification process.

All verification of Level A and B functions should be independent. Level C and lower functions do not require independent verification. Independence is needed only at the design hierarchy level at which the design is verified against the requirements. An equivalent means of independence, which addresses the issue of common mode failure, should be acceptable.

Independence is a means to address potential common mode errors that could occur when a designer verifies that the hardware item under development performs as designed, not as required. To address this concern, the responsibility for ensuring the verification process is consistent with demonstrating that the design requirements have been met should be performed with an individual, a process or a tool that is independent of the designer" (see section appendix A of reference 1).

Attributes: Verification independent of designer for Level A or B

2.16 KEY ATTRIBUTES SUMMARY.

The component attributes, which have been identified from the DO-254 objectives, can be grouped to identify key attributes, which will be considered in subsequent sections of this report (see table 3).

TABLE 3. KEY COMPONENT ATTRIBUTES

Design Assurance	Configuration Management
Component design assurance data,	Production control of parameter variation
Acceptable design assurance data for complex level A or B	Implementation, assembly and installation data
Detailed design data	Configured item
Design process data	Production variations in hardware parameters
Verification independent of designer for level A or B	Process change control
	Process change reporting
	Procurable component, (part obsolescence)
	Stable technology
Component Reliability	Component technical suitability
Failure rate data	
Reliability data	Production Practices
Component reliability	Manufacturing process control
	Manufacturing controls
Standards	Process control
	Quality control
Failure Modes	
Identifiable failure modes	Verification Testing
Anomalous behavior	Evidence that the component meets the requirements.
Identifiable unused functions	Test methodology data
List of unused functions	
Operation Beyond Mfg. Spec.	Role of COTS Tools in Design and Verification
Component rating data	Appropriate design models for formal methods
Operational environment	Assessed tools for formal methods
Environmental qualification	Assessed development tools
	Assessed verification tools
Upsets	Employ qualified verification tool
	Employ qualified design tools
Service Experience	
Acceptable product service experience	
Service experience data	
Service experience	

3. KEY ATTRIBUTES OF COTS COMPONENTS IN SAFETY CRITICAL APPLICATIONS.

3.1 PENDING GUIDANCE ON COTS COMPONENTS.

Section 11.1 of reference 1 defines COTS components as a special case of "previously developed hardware" and, as such, all guidance with respect to previously developed hardware applies to COTS components, see section 1.1 of reference 1 for further information. In addition, section 11.2 of reference 1 specifically addresses COTS components usage.

> *"As such the use of COTS components will be verified through the overall design process, including the supporting processes, as defined in this document."*

DO-254 describes design assurance objectives for airborne electronic hardware, without regard for the source of the components. It is the responsibility of the developer to provide adequate assurance for the component, be it custom designed for the application or COTS.

Section 11.2.1 of reference 1 describes several means which may establish certification credit for COTS components as follows:

> *"Certification credit may be gained by establishing that:*
>
> 1. *The component manufacturer can demonstrate a track record for production of high quality components.*
>
> 2. *Quality control procedures are established at the component manufacturer.*
>
> 3. *There is service experience supporting the successful operation of the component.*
>
> 4. *The component has been qualified by the manufacturer or by means of additional testing, which establish the component reliability.*
>
> 5. *The component manufacturer has control of the component quality level or that this is assured by means of additional component testing.*
>
> 6. *The components have been selected on the basis of technical suitability of the intended application, such as component temperature range, power or voltage rating, or that additional testing or other means has been used to establish these.*
>
> 7. *The component performance and reliability are monitored on a continuous basis, with feedback to component manufacturers concerning areas that need improvement."*

One or more of the guidance in section 11.2.1 of reference 1 is in use today, relative to critical electronics that employ plastic encapsulated microelectronics (PEMs). Section 3.8.1 Review of Best Manufacturing Practices, indicates that certain aspects of this guidance is used in industry practice, relative to ICs.

Section 11.2.2 of reference 1 identifies COTS procurement concerns which may impact design assurance. Attributes of design assurance, production control of parameter variation, and component availability over the life of the product are key concerns for COTS components. These issues may also impact the life cycle cost of the system through parts obsolescence and change impact analysis in the event that changes in the COTS component impact design assurance for safety requirements.

3.2 COMPONENT RELIABILITY.

Component reliability prediction is required for a number of hardware life cycle analyses including:

- Product selection, life cycle cost, repair level, spares and support,
- Fault Mode Effects, Criticality Analysis (FMECA), and
- System level reliability/availability/maintainability/safety.

3.2.1 Reliability Metrics Overview.

Although mean time between failure (MTBF) is by far the most commonly used measure in industry, there are many metrics in different industries. For example, automotive electronics have included specifications for R96C90 and a B50 Life of 224,000 miles. This is 96% reliability with 90% confidence and a 50% survival probability for 224,000 miles. These are stated as a "B" or "L" life at a specific time, i.e., L10 life of 300,000 hours. These numbers represent a cumulative percentage failed at a specific point in time (miles, cycles, hours, etc.). A B10 life (or sometimes referred to as L10 life) of 300,000 hours means that 10% of the products will have failed by 300,000 hours.

The electronics industry has a paradigm with only using MTBF, or a derivative such as failure rate or failures in time (FITS, the number of device failures per 1e9 device hours), as the measure of reliability. This assumes the failure distribution is exponential and may not be correct in all cases.

MTBF may be misunderstood as the life of the product. An encapsulated die may have an MTBF of 10,000,000 hours, extrapolated from accelerated test data, but this does not mean that all will survive 10M hours. It is simply a measure of product "reliability" where every 10M operating hours of a population of the IC, one will fail. If the IC failure distribution is exponentially distributed, then 63.21% of these ICs will have failed by 10M hours.

A reliability prediction from an extended operational test, life test, or durability test on a reasonable sample of product will allow making a point estimate of the MTBF of the product. It will not necessarily be the true value, another similar sample may give a different point estimate in relation to the true MTBF.

Confidence intervals allow a band or interval to be calculated around a point estimate that adds more meaning to the estimate. For example, a 90% confidence interval means that 90% of the estimates calculated in this manner from sample data will contain the true (but unknown) MTBF, while 10% will not. The higher the level of confidence, the wider will be the confidence interval. The confidence interval along with desired MTBF influences the amount of testing (hours, cycles, miles, etc.) necessary [41].

3.2.2 Benchmarking Commercial Reliability Practices.

Benchmarking Commercial Reliability Practices [42] describes an investigation by Reliability Analysis Center that included survey responses and interviews to determine the practices of

commercial companies with respect to reliability. Forty companies provided survey responses and fifteen provided two-hour interviews. The companies were selected to provide a cross section of several industry segments. Bell Helicopter, Boeing Commercial Airplane Group, Carrier Corp, Eastman Kodak, ELDEC Corp, General Motors, Motorola Cellular Phone, and Sun Microsystems were among the interviews.

Evaluation of the commercial reliability practices of these companies lead to several key observations as follows:

- Concurrent engineering is essential to being competitive.
- Thoroughly understanding the design is essential to reliability.
- Strong supplier relationships are essential. All companies interviewed have a program for reducing the number of suppliers and for certifying those suppliers. The same requirements imposed within the company are imposed on suppliers.
- Customers are not deeply involved in the design and development process. Customers tell the contractor what is needed, but not how to do it.
- Military standards, in many cases, form the basis of commercial reliability practices; however, they are often revised or modified for internal use.
- Military specifications and standards, if used without regard to their applicability or value-added, can drive up costs with no positive affect on reliability.
- Only DoD is doing and funding research needed to develop technical information included in military standards and making it available to industry. If and when commercial companies perform such research, the results are usually kept proprietary.
- Accelerated testing, Bayesian statistical methods, and other analytical methods are used extensively to supplement deterministic design.
- Designing for reliability must include the reliability of the processes as well as the product.
- Parts application is critical—select the parts most appropriate for the design and stress levels.
- Completely analyze all failures, regardless of when or where they occur in development, to identify the root cause of failure and determine the necessary corrective action, including redesign and revision of analytical tools and models.

Note that three of the eleven observations concern the use of military standards, standards which the government is no longer supporting. In 1994, the U.S. Military Specifications and Standards Reform initiative decreed the adoption of performance-based specifications for acquiring and

modifying weapon systems. This led to the cancellation of many military specifications and standards. This, coupled with the fact that the Air Force has redirected the mission of the Air Force Research Laboratory (the preparing activity for MIL-HDBK-217) away from reliability, resulted in MIL-HDBK-217 becoming obsolete, with no government plans to update it [43].

The consensus of the commercial companies ranked the importance of reliability practices in the following order of importance.

1. Failure reporting and corrective action system (including failure analysis)
2. Design reviews
3. Subcontractor/vendor control
4. Parts control
5. FMECA and other related analysis
6. Predictions, simulations, and modeling
7. Development testing, such as test, analyze, and fix (TAAF)

The consensus of these commercial companies rated Failure Reporting and Corrective Action (FRACA) as the most important reliability practice, followed by vendor and parts control. While these processes are important aspects of the hardware life cycle processes identified in DO-254, the primary focus of DO-254 is design assurance, and design assurance practices are less highly rated by consensus of these commercial companies. The commercial focus seems to be more reactive to product failures as compared to the proactive approach of implementing extensive design assurance as prescribed by the DO-254 guidance.

The commercial reliability practices, evidenced by this survey, seem to suggest that, although commercial practice values design assurance activities, the priority and extent of these activities are not aligned with the guidance of DO-254 for safety systems.

3.2.3 Tools for COTS Equipment Reliability Assessment.

Reference 44 provides a detailed survey of tools available for the selection and reliability assessment of COTS modules and equipment, which is summarized below.

- CAST

  COTS Assessment and Selection Tool (CAST) has been developed collaboratively by Lockheed Martin Federal Systems and Virginia Tech. The underlying methodology uses Quality Function Deployment (QFD) to focus on customer requirements, an analytic hierarchy process (AHP) to facilitate computation of consistent relative priorities for an attribute set, followed by a comparative analysis of potential alternatives. The tool is highly tailored to Lockheed Martin experience and is not universally applicable.

- SELECT

  Selection of Equipment to Leverage Commercial Technology (SELECT) was developed by Illinois Institute of Technology Research Institute (IITRI) for the Air Force Research

Laboratory Information Directorate. The program operates from a baseline database consisting of COTS equipment categorized by category/type, manufacturer and model number, and containing the necessary design reliability and environmental data necessary to drive the translation and risk algorithms. http://rac.iitri.org/cgi-rac/ProdDescription?SELECT

- CMMR Information Center

  The Commercial Item Military Market Research (CMMR) Information center is a newly initiated (1999) DoD information center for market research data. It will contain information generated by the Army, Air Force, and Navy on commercial products and technologies considered for use in the military.

- PATS

  The Navy Product and Technology Surveillance (PATS) is a subset of CMMR. It is a shared knowledge-based internet tool used to compile and distribute market survey and technology trending information and support COTS product selection decisions. http://pats.crane.navy.mil/

- COSIP

  The U.S. Navy Computer Open Systems Implementation Program (COSIP) has provided an initial set of engineering and analytical process tools to support the identification of candidate Non-Developmental Item/Open Systems Architecture (NDI/OSA) computer resources. http://www.nswc.navy.mil/cosip/

3.2.4 Military Demonstration Programs.

DeBusk suggests three methods to establish the reliability of a COTS component for military applications [45]:

The first method gathers and analyzes data available from manufacturers. Manufacturers of commercial equipment used in high-reliability applications, such as banks and telecommunications, perform some level of reliability analysis for their own use in identifying warrantee costs, etc. The designer should identify the source of the data used in any reliability prediction. If MIL-HDBK-217 methods were used, the results should be normalized to the appropriate environment and also adjusted for Product Service Experience (PSE) data if appropriate.

The second method is based on developing a database of experience for similar equipment. DO-254 provides guidance with respect to PSE data.

The third method builds assembly MTBFs from subassembly estimates.

The technical information available for complex COTS components may limit the level of detail achievable in the FMECA of the system. Failure modes may be limited to those exhibited at the level of the COTS component interface signal. Commercial users and maintenance manuals may provide additional failure mode information. A program for failure reporting and corrective action should be implemented. DeBusk claims "The cornerstone of COTS predictions are observed equipment MTBFs. ...measuring the observed MTBF is the only way to accurately assess the reliability of COTS equipment in military environments" [45].

Using the methods described, DeBusk predicted the failure rate for a certain ground-fixed military system consisting of 63 COTS items. Field experience with three systems monitored over 1 year tallied 43 observed failures compared to 59 failures expected.

3.2.5 Packaging Trends.

Microelectronics performance increases result from higher density and higher frequency, which cause higher power density and thermomechanical stress in the packaging of the die and it's associated interconnects. While die cracking and defects in die attachment have always been a concern, new packaging approaches and complexity pose new challenges such as solder ball fatigue and under-fill stress.

Thermomechanical stress is one of the principle roadblocks to the development of high I/O flip chip on board packages with larger than 0.5 inch dimensions [46].

Accelerated testing has uncovered failure mechanisms in PEM devices, such as corrosion at wire bond/pad interfaces and Al interconnections; however, it is difficult to screen for such defects since packages are complex and many techniques for fault identification are destructive. While a large experience base for commercial usage may be developed, it may be irrelevant to the failure mechanisms of the critical system environment.

New packaging developments pose challenges to identify the failure mechanisms and develop accelerated test techniques required to investigate reliability issues [46].

3.3 USE OF STANDARDS.

DO-254 provides guidance relative to use of standards in the hardware design life cycle; however, it does not specify particular standards. The adoption of standards seems to be left to the applicant.

The DoD is reforming the Military Specification program through migration to commercial standards where appropriate. DoD is shifting focus from "how to do it" specifications to performance requirements. Literally, thousands of military standards and specifications have been canceled or deactivated since 1994, while DoD has adopted a similar number of nongovernment standards. While the migration to performance requirements enables the use of technology in new ways, it also moves the burden of responsibility directly to the system provider/designer. Previously, the designer could have confidence that the Mil-spec part would perform reliably in harsh environments. "In the absence of Mil-Specs, a designer must determine the environment in which the electronic system will operate, establish that a particular

commercial IC will operate reliably in that environment, and plan for parts obsolescence" [9]. The designer now must establish in-house standards and also evaluate the in-house and industry standards which may be used by suppliers.

Standards selection poses several challenges to the designer [4]:

1. Many of the military specifications are being canceled, or replaced by guidance documents;

2. Commercial standards are generated by several organization;

3. Exact equivalent commercial standards do not necessarily exist;

4. Lack of assistance from qualified technical resources, and

5. The commercial standards change relatively fast.

Sixteen organizations identified by reference 4 represent a partial list of organizations involved in commercial standards. Reference 4 suggests a table of commercial standards which are almost equivalent to military standard counterparts. A survey of worldwide standards relevant to the use of programmable electronics in safety-related applications is documented in reference 47, where a total of 476 standards were identified covering 15 countries and seven industries. See table 4 for the specification transition from military to almost equivalent commercial.

STANDARDS GENERATING/SUPPLYING ORGANIZATIONS [4]

- The Institute For Interconnecting and Packaging Electronic Circuits (IPC)
- Accredited Standards Committee (ASC)
- American National Standards Institute (ANSI)
- Defense Standardization Program (DSP)
- Communications Standards Review (CSR)
- Data Interchange Standards Association (DISA)
- Department of Energy (DOE)
- Electronic Data Interchange Standard (EDIS)
- Institute of Electrical and Electronic Engineers (IEEE)
- National Fire Protection Association (NFPA)
- National Institute of Standards and Technology (NIST)
- National Standards Systems Network (NSSN)
- Optical Society of America (OSA)Institute of Electrical Engineers (IEE)
- Underwriters Laboratory (UL)
- National Electrical Manufacturers Association (NEMA)
- VITA (VME bus International Trade Association) Standards Organization (VSO)
- FOR MORE INFO: http://www.eia.org/eng/linksdo.htm http://www.acq.osd.mil/es/std/ stdhome.html

TABLE 4. SPECIFICATION TRANSITION—FROM MILITARY TO *ALMOST* EQUIVALENT COMMERCIAL [4]

SUBJECT	MIL SPEC TO	COMMERCIAL SPEC
• Quality	MIL-Q-9858	ISO-9000 & ASQC-92 Series
• Inspection System	MIL-I-45208	ISO-9000 & ASQC-92 Series
• Design - Rigid	MIL-STD-275E	IPC-D-275 (draft -IPC 2221/2222)
• SM Land Patterns -	-	IPC-SM-782A
• Flex Circuit	MIL-STD-2118	IPC-D-249 (draft - IPC 2221/2223)
• Rigid Flex	MIL-STD-2118	IPC-D-249 (draft - IPC 2221/2223)
• MCM Laminate -	-	IPC-MC-790 (draft - IPC 2221/2225)
• Documentation	MIL-STD-130 & 275E	IPC-D-325A
• Rel Des Guideline	-	SM - IPC-D-279
• Perm Solder Mask -	-	IPC-SM-840C
• Fab - Rigid PWB	MIL-P-55220E	IPC 6011;6012 (draft)
• Flex & Rigid/Flex	MIL-P-50884C	IPC-RF-245 (draft - IPC 6011/6013)
• Assembly - Rig, Flex, Ri/Flex	MIL-C-28809B	PC-CM-770D (OLD)
• Soldering	MIL-STD-2000A	J-STD-001B
• Components Handling	MIL-D-3464	IPC-SM-786A (OLD) J-STD-020A
• Comp – Solderability	MIL-STD-202	J-STD-002
• PWB Solderability	MIL-P-55110	J-STD-003
• Fluxes	MIL-F-14256	J-STD-004
• Solder Alloy	QQ-S-571	J-STD-005
• Conformal Coating	MIL-I-46058	IPC-CC-830 (OLD)
	MIL-STD-2000A	IPC-CC-830A

NOTE: IPC Standards are also changing.
CONTACT: http://www.ipc.org for current information on standards.

3.3.1 Standards: Safety Verification/Validation.

Reference 19 describes an in-depth survey, reported on in 1995, which reviewed over 60 standards documents which were either adopted or under development with respect to safety verification/validation standards/guidelines for computer-based systems. The purpose of the survey was to establish a basis for development of a specific industry approved methodology for ensuring the safe operation of safety critical computer-based subsystems to be adopted by the Federal Railroad Administration (FRA). An extensive summary of each document reviewed is provided in reference 19.

Trends identified by the survey model many of the objectives of DO-254 and are listed below.

- Safety assessments are being required/recommended throughout the development cycle from conceptual design through final stages.

- Hazard analyses and risk assessments are being required/recommended in early design stages.

- A wide mix of analysis and testing techniques are being required/recommended, with no clear methods dominating.

- No trend exists for requiring versus recommending/suggesting possible verification/ validation techniques.

- Emphasis has been on software, but is now becoming system focused.

- Formal methods for software development are gaining acceptance and are being recognized as useful techniques.

- Methodologies are required/recommended separate safety-related development and assessment processes/activities for software.

- Methodologies are required/recommended independent safety assessments.

- Methodologies are required/recommended the establishment of quality assurance plans in addition to safety plans.

- Emphasis appears to be placed on proof-of-safety requirements—what process, activities, and documentation has to be performed/submitted to adequately demonstrate the safety of the system.

3.3.2 Quality Manufacturers List.

DoD created the Quality Manufacturers List (QML) (table 5) program in 1989 to a shift away from the Qualified Parts List (QPL) program. The QPL program focused on "how to do it" guidance for achieving quality parts. QPL provided designers with parts of known quality and reliability in harsh environments; however, new technology was introduced to the QPL years after commercial introduction, if at all. Improved generation logic implementations which incorporated latch-up mitigation and electrostatic discharge (ESD) immunity were not available on the QPL. The QML focuses on a manufacturer's ability to design and produce parts that consistently meet performance specifications and to maintain consistent quality as they improve their production processes [9]. Manufactures are audited and certified for compliance with the MIL-PRF-38535 performance specification, for the production of certain types of parts.

The QML program allows manufacturers to eliminate end-of-line testing of individual devices, in the case where analysis of manufacturing and testing data show the end-of-line testing to no longer be necessary [48]. QML allows for incorporation of commercial best practices and the use of commercial production lines, while still providing a level of configuration control, device traceability, and other special services required for critical microelectronics.

A Process Conformance Report is provided by one major QML supplier that indicates to the customer which production processing steps were actually undergone by the delivered device. The user of the component must evaluate the effect of any production process change on the OEM application. Mechanisms for communication of COTS process changes between the

COTS supplier and the OEM, are often established by policy, contract, or certified supplier program agreements. Process changes may present challenges to OEMs who have qualified COTS devices for operation outside manufacturer's specifications.

TABLE 5. QML MANUFACTURERS PER QML 38535 REV 012

QML Vendor	Qualified Devices
Actel	Field programmable gate array and rad hard FPGA
AlliedSignal MTC	Standard cell and full custom ASIC
American Microsystems, Inc.	Gate arrays, standard cells
Analog Devices	Data converters, op amps, analog and DSPs, sensors, references, switches, multiplexers
Austin Semiconductor	Memory products (SRAM, DRAM, VRAM) and custom products
Cypress Semiconductor	SRAM, PROM, EPROM, PLD, logic, clocks, DCOM
DPA Components International	All
Golden Altos Corporation	Na
Honeywell SSEC	Core product types (CPT):[SRAM, ROM, gate array ASICs, full custom]; RICMOS IV: CPT; SOI IV: CPT, memory MCM, SOI
IVE	Memory
IDT	Microprocessors, SRAM, logic, micro processors
Intersil, Corp	Memory, logic, switches, timers, microprocessors, micro-peripherals
Lansdale Semiconductor, Inc	Logic, gate array, memory, microprocessors, others
Linear Technology	Linear integrated circuits
Linfinity Microelectronics, Inc.	Regulators, op amps, comparaters, sense amps, drivers, transistor arrays
Lockheed Martin S E & C	SRAM, logic, VCOS memory and logic, microproc., cust. & gate array ASICs
MHS S.A.	SRAMs, ASICS, memories
National Semiconductor Corporation	Analog, logic, memory, interface
Pantronix Corporation	All (assembly and test house only)
Qualified Parts Laboratory	Bipolar memory, linear, microcontroller, SRAM, PROM, EPROM, PLD & logic
Sarnoff Corporation	TTL, CMOS, CMOS4000, HiNil, PMOS, NMOS, ECL
Signal Processing Technologies	Analog to digital converters, digital to analog converters
Siliconix	Analog switches, analog multiplexers, power drivers, video switch
Texas Instruments	Logic, memory, DSP, PAL, ASIC, op amps, comparators, voltage regulators, data converters, data transmission drivers
Thomson CSF	Microprocessors, microcontrollers, memory
Unitrode Corporation	Pulse width modulators, regulators, diode arrays, controllers, drivers
UTMC Microelectronics Systems Inc.	Memory, CMOS gate array, linear bipolar
White Electronic Designs Inc	SRAM
Xilinx Incorporated	Logic, gate arrays, FPGA, EPROM, SPROM

3.4 FAILURE MODES.

Section B-2.2 of reference 1, FFPA Data, provides guidance as to the information that should be provided by the applicant for level A and level B hardware. In part, section B-2.2 of reference 1 requires that the data should:

> *"Identify the FFPs, the effects of their anomalous behavior or functional failure and decomposition level in the design hierarchy to which the analysis was performed and the type and location of the acceptable assurance data that should be available."*

Next generation microelectronics may exhibit new failure modes brought about by several technology trends being pursued to increase the performance/cost ratio of the devices. Smaller feature size allows increased density and complexity, however, effects such as higher transistor leakage currents, transistor threshold voltage variation, and cross-talk may contribute to lower reliability. Increased complexity requires additional interconnects, perhaps on seven-to-eight levels, which pose issues in contact and via failure, cross-talk, and effectiveness of front-side fault analysis techniques currently employed [49].

Front-side fault analysis techniques will be unable to detect some defects, since they will be invisible to the optical techniques currently employed, either due to small feature size or obstruction of view. The front-side access to the circuitry will be severely impeded by the dense wiring and multiple interconnect levels. New packaging techniques, such as flip-chip, inhibit fault analysis via currently used techniques. Further, the tools currently used for front-side analysis will not be effective for backside analysis [49].

Microelectronics design must make provisions for failure analysis by incorporating features such as design for test techniques, internal e-beam probe points, and navigation marks [49].

3.5 OPERATION BEYOND MANUFACTURERS SPECIFICATIONS.

As previously defined, ROTS and MOTS are terms sometimes applied to components that are employed outside the manufacturers environmental specifications. These components have been "uprated" by the OEMs who employ extra testing and part screening to establish that components have extra margins that allow operation at higher temperatures, under radiation conditions, or other conditions which may be required for critical applications [4 and 6]. Manufacturers discourage use of their products in this way, disclaim all liability, and generally will not cooperate with OEMs who practice uprating.

Reference 4 provided the following summary of helpful guides for component uprating which they compiled from at least 15 organizations in four workshops:

- Determine the "real environment" of the system.
- Maintain maximum margin (safety factor) during design optimization.
- Select and certify a supplier.
- Do not count on receiving any help from the commercial suppliers.

- Use supplier's test data or actual test data to determine the capabilities of parts.
- Analyze design rules—they may not be the same as the spec sheets.
- Use the same manufacturer, same fabrication, and same date code when possible.
- Just-in-time is not necessarily compatible with uprating.
- Do not burn-in.
- Resistors in plastic packages change value when thermal cycled.
- Involve customer and suppliers early in design.
- Marking of screened parts is important for field repair.
- Control environmental impact through external means.
- Take full ownership of the product.

OEMs may invest significant effort in qualifying COTS components for uprated operation. In some cases, the die used for PEMs is produced by the same production line as the die packaged in hermetically sealed ceramic for high-temperature operation. Design rules for high-temperature (125°C) operation were once the standard, however, new market pressures have encouraged some microelectronics designers to switch to lower temperature design rules. IC performance parameters may be found to deviate widely from predictions extrapolated and from normal range performance curves. After extensive measurement of the actual at-temperature performance, these characteristics can be determined and addressed in the circuit design.

The OEM must implement a strategy to address supplier process changes or variations which may impact the characteristics which have been qualified. Supplier agreements and extensive unit tests are two approaches. Major suppliers such as Motorola, AMD, and Intel no longer support the extensive testing required, and as a result, third-party test houses have emerged to meet this need for OEMs who do not wish to maintain an in-house capability. They supply testing services for small batches of components to a variety of customers, providing the specialized skills and equipment required. Third-party test capabilities include thermal cycle, 160-hour burn-in, and electrical test at-temperature [50].

3.6 SINGLE-EVENT UPSETS.

Studies completed in the early 1990s, clearly correlated measured in-flight shutdowns with atmospheric neutron flux and laboratory data [51]. Random access memory components have been the traditional concern, which has been addressed by error detection and correction circuitry. However, other parts are potentially susceptible as well, including microprocessors, linear devices, opt-couplers, and even newly emerging micro-electro mechanical systems (MEMS) [52].

Radiation effects and testing programs are being carried out at the jet propulsion laboratory in order to gain radiation hardness assurances necessary to introduce COTS components into National Aeronautics and Space Administration (NASA) space systems. The rapidly changing technologies of the commercial sector, coupled with the disappearance of suppliers for radiation-hardened devices, provide significant challenges. Device scaling effects, driven by commercial market pressures, "often result in increased vulnerability to radiation. ...the introduction of new and emerging technologies that promise greater performance without increased power, weight, or

volume may have completely unknown radiation effects behavior that must be established through testing" [52].

While a detailed evaluation of single-event effects testing is beyond the scope of this report, the following references provide a glimpse of the types of device testing being undertaken in an attempt to gain assurances in this challenging technical area [51, 52, 53, 54, 55, 56, and 57].

Actel discusses design techniques, for use with their FGPAs, which provide tolerance to single event upset in application notes [58 and 59].

3.7 PRODUCT SERVICE EXPERIENCE.

Product "Service experience may be used to substantiate design assurance for previously developed hardware and for COTS components" (see section 11.3 of reference 1). PSE may be an important assurance strategy for COTS components in some applications. In the DoD's transition to COTS components, a number of military demonstration programs are being conducted which may help establish PSE. Sections 11.3.1, .2, and .3 of reference 1 provide guidance as to the criteria that establishes if PSE data is acceptable, the assessment process to determine if PSE data is acceptable, and the data which should be provided by the process. The PSE must be shown to be relevant to the application at hand, with special focus on the in-service exercising of the particular hardware functions associated with the design assurance to be substantiated.

As previously noted, DeBusk [45] claims "The cornerstone of COTS predictions are observed equipment MTBFs. ...measuring the observed MTBF is the only way to accurately assess the reliability of COTS equipment in military environments." DeBusk points to a design flaw in a COTS assembly which resulted in several field failures. After discussion with the COTS supplier, it was determined that the flaw had been already identified and corrected during the course of commercial practice. While COTS advocates would point to this type of flaw identification and corrective action as contributor to quality components, the fact that flawed components were actually fielded is a significant concern for critical systems and the main focus of DO-254 pending guidance.

COTS supplier programs for failure reporting, corrective action, and root cause analysis, both within the production process and for components in service, should be an important aspect of airborne certification programs conducted by the OEM. While no data was discovered on service history, there is evidence of failure reporting programs at both OEMs and component suppliers.

3.8 PRODUCTION PRACTICES.

3.8.1 Review of Best Manufacturing Practices.

The Best Manufacturing Practices Center of Excellence is a partnership formed by the Office of Naval Research, the U.S. Department of Commerce's Bureau of Export Administration, and the University of Maryland's Engineering Research Center, http://www.bmpcoe.org/index.html. The Center identifies and documents industry best practices through surveys of industry

companies. The surveys provide an insight to successful approaches and current trends. The following observations are drawn from review of surveys for the following companies:

- Litton AMECOM Division—College Park, MD
- Litton Guidance & Control Systems Division—Woodland Hills, CA
- Harris Semiconductor (Intersil Corporation)—Palm Bay, FL
- ITT Industries Aerospace/Communications Division—Fort Wayne, IN
- Texas Instruments Semiconductor Group—Midland, TX
- Texas Instruments, DS&EG (Raytheon TI Systems)—Dallas, TX
- Westinghouse Electronic Systems Group (Northrop Grumman Corp.)—Baltimore, MD
- Hamilton Standard Electronic Manufacturing Center—Farmington, CT
- Kaiser Electronics—San Jose, CA
- Raytheon Missile Systems Company—Tucson, AZ
- Raytheon Missile Systems Division—Andover, MA
- McDonnell Douglas Aerospace-St. Louis (Boeing Aircraft and Missiles)—St. Louis, MO
- Northrop Grumman Corporation—El Segundo, CA
- Rockwell Collins Avionics and Communications Div. (Rockwell Collins, Inc.)—Cedar Rapids, IA
- Lockheed Martin Electronics and Missiles—Orlando, FL
- Lockheed Martin, Government Electronic Systems—Moorestown, NJ
- Lockheed Martin Tactical Aircraft Systems—Ft. Worth, TX

In the early '80s, many of these companies instituted extensive part screening programs which tested each part over temperature and vibration conditions to identify defective parts. Experience during the '80s, was that many boards were failing functional tests due to part defects and part screening and was effective in increasing the yield at the board level and reducing costly troubleshooting and rework.

Over the last 10 years, IC manufacturers' processes were improved such that process yields may approach 100 ppm. Some OEMs are therefore eliminating the costly in-house part screening tests and instead establishing supplier qualification programs. The OEMs approve suppliers who demonstrate the manufacturing processes necessary to reliably provide defect-free parts. The supplier program must monitor and control key part characteristics using Statistical Process Control (SPC) methods, have both corrective action and continuous improvement plans in place, and be committed to total quality management.

At some manufacturers, functional testing at the board level is being replaced by in-circuit or bed-of-nails testing. With part quality being provided through supplier certification programs, in-circuit testing identifies the few defective parts while exercising the board as well. In-circuit testing is not only an effective replacement for board-level functional testing, but also offers significant cost savings due to reduced test development cost, reduced test fixture development cost, and reduced test cycle times.

Boundary scan test (BST) is another trend seen in several best practice surveys. BST combines digital circuit design, design for test, and prototype test functions. The BST circuitry is resident

within the microelectronics and is exercised by PC-based test systems running COTS software tools. The BST approach replaces expensive automated test systems and, in one example, reduced trouble shooting cycle times by a factor of 8:1. BST is further discussed in Section 3.10.2, Verification Testing.

Other best practices address failure reporting and change control processes, both in-house and through supplier interactions. The decline of sources for Mil-spec components and parts obsolescence are issues for the industry raised in some surveys. Some manufacturers implement ASICs which are form, fit, and function compatible with parts that are no longer available. The use of plastic encapsulated microelectronics (PEMs), where acceptable, has provided significant cost savings, which many manufacturers attribute to the use of COTS components.

3.8.2 Review of Quality and Reliability Programs.

Several major supplier quality and reliability programs were reviewed. Extensive programs are in place and documented as supplier policy. Many are modeled after ISO9001 requirements, which cover the entire manufacturing operation, including the 17 points below:

- Management Review
- Quality Systems
- Contract Review
- Document Control
- Purchasing
- Product Identification and Traceability
- Process Control
- Inspection and Test
- Inspection, Measuring, and Test Equipment
- Inspection and Test Status
- Control of Nonconforming Product
- Corrective Action
- Handling, Storage, Packing, and Delivery
- Quality Records
- Internal Quality Audits
- Training
- Statistical Techniques

3.9 CONFIGURATION MANAGEMENT.

3.9.1 Pending Guidance on Configuration Management.

Section 7 of reference 1, describes the configuration management process. Process control, process change control, and process change reporting are attributes identified. Selected excerpts follow.

> *"The Configuration Management Process is intended to provide the ability to consistently replicate the configuration item..."* (see section 7.0 of reference 1).

"Baselines should be established for configuration items used for certification credit. The baseline may be a configuration item, a previously certified hardware item, or a COTS component. Once a baseline is established it should be subject to change control procedures" (see section 7.2.2 of reference 1).

"Change control should ensure that the impact of the change is assessed to determine the effect of the change on the outputs of the processes and that the output data is updated.

Note 1: Some or all of the activities of the processes may need to be repeated from the point at which their outputs are affected.

Note 2: It should be recognized that a change to the manufacturing tools, technology processes or external components may impact the design" (see section 7.2.4 of reference 1).

Configuration management and change impact assessment may become issues if changes, which occur in COTS components, impact safety requirements. The design processes and assurances impacted by any change must be evaluated to determine if the change effects the ability to meet the safety requirements.

3.9.2 Parts Obsolescence.

The expected life cycle of both military and commercial avionics (10-20+ years) is diverging significantly from the 3- to 5-year life cycle of commercial microelectronics, as previously discussed in Section 1.2.3 COTS Market Trends. Suppliers are choosing to leave the military component market. Parts obsolescence is a major challenge to the DoD as well as commercial OEMs and is expected to continue for many years.

Approaches to dealing with parts obsolescence are expensive and cumbersome. They include stock piling of original parts, transfer of technology and tooling to third-party suppliers, re-engineering of the obsolete microcircuit, or redesign of parts or all of the subsystem [9].

Stockpiling of original parts, or lifetime buys, is a traditional approach that is very expensive and can result in millions of dollars worth of components kept in inventory, with only a fraction ever being used.

Third-party suppliers or after-market manufacturers may continue to provide components if adequate technical information is available. Escrow of design data is sometimes employed to circumvent parts obsolescence if the original supplier leaves the market. As original suppliers move to next generation processes, the tooling required for manufacture must be reclaimed by third-party suppliers to continue production. There is some question whether the third-party suppliers are able to maintain the same quality control of the processes in low-volume runs, as the original suppliers could in large-volume runs. One after-market supplier proudly claims to be "leaders on the trailing edge of technology," http://www.rocelec.com/default.htm.

Re-engineering of the microelectronics includes emulation, reverse engineering, and retargeting. Emulation is the process of developing a form, fit, and function replacement for the obsolete component. The General Emulation of Microcircuits Program supports this function for the DoD. Retargeting involves the capture of the functionality of the microcircuit in a software language or model, which can then be retargeted at state-of-the-art processing techniques [60]. Reference 61 describes a hardware modeling approach to ASIC redesign for direct component form, fit, and function replacement where the target ASIC is exercised by a series of test vectors which allow formulation of a Very-High-Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL) design model for the targeted ASIC. Once the VHDL design model is verified against the actual ASIC, the VHDL can then be retargeted to a new ASIC design process or to an FGPA implementation.

3.10 VERIFICATION APPROACHES.

3.10.1 DO-254 Pending Guidance for Verification.

Section 6.2 of reference 1 describes the verification process as follows:

> *"The verification process provides assurance that the hardware item implementation meets the requirements. Note 1: Safety aspects of hardware design take the form of safety requirements to be met by the hardware implementation."*
>
> Objectives for the verification process include the following:
>
> *"1. Evidence is provided that the hardware implementation meets the requirements."*
>
> *"2. Traceability is established between hardware requirements, the implementation, and the verification procedures and results"* (see section 6.2.1 of reference 1).
>
> However,
>
> *"It is not intended to require traceability to detailed components (for example: resistor, capacitor and gate) unless required for safety considerations"* (see section 6.2.2 of reference 1).

Section 6.3 of reference 1 describes three methods that may be applicable to verification: test, analysis, and reviews. Verification testing and role of COTS tools in analysis for verification are discussed in sections 3.10.2 and 3.11. The role of reviews will not be discussed except to provide the following definition:

> *"A review is a qualitative method for evaluation of the plans, requirements, design data, design concept or design implementation"* (see section 6.3.3 of reference 1).

3.10.2 Verification Testing.

3.10.2.1 DO-254 Pending Guidance for Test.

> *"Test is a method that confirms that the hardware item correctly responds to a stimulus or series of stimuli. Examples of tests are functional test on the hardware item, system bench test, system validation facility test, and aircraft test." 'When it is not feasible to verify specific requirements by exercising the hardware item in its intended operational environment, other verification means should be provided, and justified." "...testing associated with certification credit requires a configured item." "Environmental qualification test requirements are part of these requirements"* (see section 6.3.1 of reference 1).

3.10.2.2 Supplier/OEM Role in Testing.

Over the last 10 years, testing approaches for properly detecting part defects has been shifting from the OEM manufacturer to the microelectronics supplier.

Part screening at the OEM manufacturer was the traditional approach; however, the OEM may have limited design information with respect to the microelectronics and, therefore, test development may be challenging. Maintaining testing capability at the OEM is expensive in terms of both equipment and skilled staff.

The microelectronics supplier has the design information and resources needed for testing. Test vectors and methods are native to the supplier's processes and test equipment; however, the suppliers may be detached from the functional implementation of the silicon, particularly in the case of ASICs, and may be under commercial market cost pressure to reduce the time and costs associated with end-of-line testing.

For critical applications, the tradeoff between testing at the COTS supplier and testing at the OEM is a challenging issue, which is becoming more important as microelectronics become more complex. As complex microelectronics move towards SOC, end-of-line testing, at the supplier's facility, is becoming a significant cost driver in terms of design for test, test development, test equipment cost, and test cycle time. For complex commercial microelectronics, the cost of end-of-line testing is approaching the cost of producing the silicon in some cases, and design verification generally accounts for 50% or more of the design cycle [62].

3.10.2.3 Testing Methods.

Behavioral or functional testing exercises the device in the way the designer intended it to operate. During the course of the design, during functional simulation, the designer generated a set of input test vectors and examined the outputs for proper operation. In behavioral testing, an analogous subset of input test vectors is used and the results of the device outputs are correlated to the expected results. Fault coverage is limited by the number of test vectors. Software tools can be used to determine the fault coverage which usually ranges from 60 to 80 percent. This

type of testing is done at system speed and, as such, is able to identify faults which are undetectable by other means.

Built-in self-test (BIST) can be used for both manufacturing and system level testing. Hardware for both a test signal generator and a response analyzer are incorporated in the chip's design. This technique is particularly suited to memory blocks where fault coverage of over 95% can be achieved with only a few additional gates. The chip will operate in normal and test modes. Development of the proper test vectors and signature responses requires a detailed analysis of the design. Test patterns can allow exhaustive testing, however, a much smaller set of prestored patterns is usually employed. Design tools to automatically generate BIST circuitry and test vectors are becoming available. Using of BIST may incur a 5% to 40% silicon overhead on each chip; however, it significantly reduces the need for complex and expensive automated test equipment. While BIST alone is not effective for testing of combinational logic, it can be used in combination with a scan-based architecture. One study predicts that 90% of designs will incorporate BIST by 2010 [63].

In Scan test, the chip also has two modes: normal and test. The ASIC is designed to incorporate control and monitoring of all the state devices such as flip-flops, registers, counters, etc. Two serial shift registers are incorporated: one for input test vectors and one for output of captured data. Scan test provides high fault coverage and good fault isolation but is applicable to synchronous logic only. A large number of test vectors is required, and costly test equipment is needed to handle the input and output data. The testing is slow due to the large amount of data and the need to serially load and unload the shift registers. Many design tools are available and the technique requires approximately 20% silicon overhead. Partial scan uses a selected subset of the full scan inputs and monitor points to provide partial fault coverage, as determined through fault coverage analysis, at reduced test time.

Boundary Scan Test (BST) is a test approach defined by industry standard IEEE 1149.1 in terms of architecture, protocol, and even a language for test equipment programming. Each device I/O pin is connected to a register cell, which is controlled by on-chip circuitry for test operations. The ASIC incorporates a standardized 4- to 5-pin Test Access Port (TAP) through which the test modes are controlled using low-cost PC-based test equipment. Boundary scan is becoming a de facto standard interface for in-system test and fault diagnosis. It can also be used to test interconnections between ICs on a printed wiring board, allowing system testing in fully working systems. Since BST is not an at-speed test, only static faults such as "stuck-at" can be detected and, while fault coverage is low, silicon overhead is also low at about 5%. BST was mentioned as a best practice by several of the airborne systems vendors reviewed. IEEE P1149.4 Working Group is developing a standard to extend boundary scan to analog structures [64].

Iddq testing measures the device current (I) which flows from the device power supply pin (dd) in a quiescent (q) condition. The inputs are cycled by test vectors designed to toggle each logic state in the device, and the measured Iddq is compared to the expected value for each test vector. The approach is highly recommended for Complimentary Metal Oxide Semiconductor (CMOS) logic devices and is able to detect both faults and leakage currents that are indicative of future failures. Ten percent of all ASIC faults can be detected only by this technique. A small silicon overhead may be incurred by incorporating an on-chip current sensor circuit. The state of the

logic must be held static while the precision current measurement is made, resulting in slow to moderate test vector frequency. Again, the fault coverage may be traded for test cycle time. The use of only 20 test vectors, which is typical of commercial production testing, may not provide adequate coverage for critical systems.

The effectiveness of Iddq testing will be challenged as the industry moves to smaller scale devices, since cell leakage currents will be reduced. Research efforts at the EQRC, Sandia [65] are developing alternative methods based on Transient Power Supply Voltage Analysis for detecting similar faults.

References 66 and 67 provide in-depth discussions of the test methods discussed above and are the general references for this testing methods section.

A major automotive supplier described an interesting test technique where "part average test limits" are imposed on each die. In this test technique, a distinct distribution of values is established for each measured characteristic. The test results for each die are compared to average test results for it's seven nearest neighbors on the wafer. Dies, which do not meet the part average test limits, are rejected. This statistical test technique of each die has been shown to reduce in-house part rejection by a factor of 10 and warrantee repair rate by 50% [17].

3.10.2.4 Other Testing Findings.

- Avionics Temperature Environment

  Reference 68 provides a discussion of field data taken to characterize the thermal environment seen by commercial avionics. It was concluded that the commercial aircraft environment, as defined by the Institute for Interconnecting and Packaging Electronic Circuits (IPC), is realistic for flight deck-mounted avionics, while it is "too benign for EE bay equipment design."

- Device Burn-In

  Device burn-in is a widely accepted practice used to identify devices of marginal reliability through accelerated testing at elevated temperatures. Typically, the devices are screen tested at 125°C for 160 hrs and tested at -40°, 25° and 125°C per MIL-STD-883. It is widely accepted that this screening would reduce infant mortality failures and increase the reliability of the fielded system. Reference 69 disputes the need for device burn-in testing due to the high quality of devices produced by current, quality-controlled production processes. Supporting field data is discussed. They further assert that the burn-in process may have detrimental effects on the reliability of devices put in the field.

Ball Grid Array Reliability

The reliability of Ball Grid Array (BGA) packages is discussed in reference 70, where joint failure mechanisms have been evidenced during thermal cycle testing.

3.11 ROLE OF COTS TOOLS IN VERIFICATION ANALYSIS.

3.11.1 DO-254 Pending Guidance for Analysis and Simulation.

> *"Analysis is a detailed, repeatable, analytical method for evaluation of specific hardware item characteristics to demonstrate that a specific requirement is met. Examples of analyses are stress analysis, design margin analysis, common mode failure analysis, worst case analysis and test coverage analysis. Service experience may provide data for various analyses. Note: As the complexity of the hardware design increases, it is advantageous to make use of computerized tools such as simulation to verify requirements and implementation of the design"* (see section 6.3.2 of reference 1).

> *"Analyses may include a detailed examination of the functionality, performance, traceability and safety implications of a hardware item function and its relationship to other functions within the airborne system or equipment. Analysis activities alone or in combination with other verification methods provide evidence that a requirement is correctly implemented. Analysis should be based on data provided by the design process, service experience, or other available databases"* (see section 6.3.2 of reference 1).

> *"Simulation is an important design analysis tool both for visualization of circuit operation and for higher level functional operation. Simulation can be used to analyze the impact of production variations in hardware parameters that would be difficult to do using other verification means and thus build confidence in reduction of design errors affecting safety due to these variations. Since the results depend on the models and scenarios employed, simulation results alone cannot be used for the purpose of certification credit without supporting evidence of their validity"* (see section 6.3.2 of reference 1).

3.11.2 DO-254 Pending Guidance for Tools.

During the hardware design life cycle, both hardware and software tools may be employed in various cycle processes. DO-254 identifies two types of tools: design tools and verification tools (see section 11.4 of reference 1).

Design tools are tools used to generate the hardware design or the hardware item. As such, errors in design tools could introduce an error in the hardware item.

Verification tools are tools used to verify the hardware item. As such, errors in verification tools may cause the tool to fail to detect an error in the hardware item.

An assessment of each tool that will be used in the design cycle should be performed to determine if the tool is "capable of performing the particular design or verification activity to an acceptable level of confidence for which the tool will be used" (see section 11.4.1 of reference 1). Section 11.4.2 of reference 1 provides a flow chart to aid in assessment of a tool

that poses a series of questions. If the output of the tool is independently verified by another means, no further assessment is necessary. "If the tool is used as a design tool for hardware implementing a Level C function or is used as a design or verification tool for hardware implementing a Level A or B function, then further assessment is needed." "When it is possible to show that the tool has been previously used and has been found to produce acceptable results, then no further assessment is necessary." However if no such relevant history can be evidenced, then the tool must under go "Basic Tool Qualification" which includes tool configuration control, a tool problem reporting process, and a process "to confirm that the tool produces correct outputs for its intended application using analysis or testing." In addition, for tools being used as "a Level A or B hardware design tool", further "Design Tool Qualification" must be done. Section 11.4.2 of reference 1 describes the data that should be provided which includes "Details of tool qualification, including the requirements used in testing, the test procedures, expected results, analysis procedures used to interpret and supplement the test results, and how independence is established."

> *"Design Tool Qualification. Qualify the Level A or B tool as a design tool using the strategies described in Appendix B of this document, the tool qualification guidance of RTCA DO-178B / EUROCAE ED-12B (or later version) for software development tools, or other means acceptable to the certification authority. Independence of this activity from the tool development should also be established.*
>
> *Note: Specific guidance for Level A and B design tool qualification is not provided here because of the variability of the circumstances of the tool usage, technology involved, visibility of the tool's implementation and life cycle data, and other factors. Using such a design tool without independent assessment of the tool's output or establishing relevant history is discouraged, as it may prove to be a task as challenging as the development of the hardware for which the tool is proposed to be used"* (see section 11.4.2 of reference 1).

3.11.3 Another Guidance Discussion on Tools.

Guidance for the Adoption of Tools for Use in Safety Related Software Development [71] provides a good discussion of the title issue. Selected observations follow:

- Tools from different suppliers may exhibit incompatibilities.
- Few independent sources of information and advise on commercial tools are available.
- It is now generally recognized that there is a decreasing ability to 100% test/validate/evaluate complex systems. This equally applies to commercial tools and other methods of assessment must be used.
- The information needed to effectively evaluate a tool for use in development of a critical system maybe company proprietary.
- As upgrades occur for commercial tools, the tools may need to be re-evaluated.

Reference 71 offers the following series of questions relative to commercial development tools:

- Can the supplier provide evidence of use in safety-related systems (SRS)?
- Have any third-party assessments been carried out?
- Does the supplier make any written commitments regarding SRS?
- What software techniques were used to develop the tool, are used within the tool?
- Can the supplier show evidence of an effective quality system?
- Does the supplier inform all customers of faults found by customers?
- Is the performance history of the tool auditable?
- Is the tool stable enough to enable a certification exercise to be worthwhile? [71]

3.11.4 Overview of the Role of Tools in Design and Verification.

As the complexity of microelectronics continues to increase, the designer is faced with increased pressure to improve his/her productivity. The engineering design automation (EDA) tools available have fallen behind; however, the current move towards System On a Chip (SOC) designs, which may incorporate close to one million gates, has sparked the development of a new wave of EDA tools that will enable the trend to a more and more complex microelectronics development. At a recent EDA tool conference, Intel's president issued a challenge to EDA tool vendors to step-up to the industry need for more capable tools and methods. Numerous tools are coming to market which are targeted at various segments of the design, verification, and design for test processes required for successful first silicon in SOC applications.

The complex microelectronics chip is expected to respond in appropriate fashion to any combination of inputs. As the complexity has increased, the number of input combinations has essentially become infinite, and there is no way to test all combinations of inputs and memory values [72]. In the traditional approach to design verification, designers conceive tests to exercise the inputs and evaluate the outputs for proper responses. This activity is labor intensive and to some extent "hit or miss." Exhaustive testing is not practical in terms of labor or simulation resources. The consequences of failure to identify design flaws, however, can result in reworked designs and additional chip prototype cycles which can take up to 4 months, resulting in millions of dollars in added labor and lost revenues [72]. For critical systems, the consequences of design flaws go beyond financial losses.

The urgent need for advanced EDA tools in the commercial sector has spawned the development of both design tools and design for test (DFT) tools. Traditionally, the design and test developments were relatively isolated processes with different purposes. The design process was concerned with proper behavior or functionality, while the test process was concerned with identifying failures in the manufactured microcircuit. The complexity of current microcircuits would require a prohibitive number of test vectors to verify a design and an equally prohibitive number of test vectors to identify all possible manufacturing defects. In many situations, the design must be modified to allow detection of certain faults. Developers must move towards integration of design and DFT at the onset of a project.

EDA tools are coming to market, which aid designers in the numerous aspects of the design process. These tools are currently supplied as separate, add-on tools which interface with the

base design package, forming a suite of design tools. Each tool is designed to aid in a specific, limited aspect of the design cycle, for example simulation fault coverage. Coverage tools monitor the designer's simulation tools as the designer attempts to verify the design through a series of test vectors. The coverage tool tracks the portions of the design which are being exercised by the test vectors and guides the designer to untested portions which need additional verification. The coverage tool is one of a number of specialized tools the designer could employ in the design verification process. No one tool covers all aspects of the verification process, and the designer must understand the proper application and limitations of a particular tool and also how the tool interfaces and interacts with other tools, often from a variety of vendors. Verification of a design is traditionally done through simulation; however, a second approach, formal verification, is currently growing in usage and tool support.

Simulation executes a model of the design, typically HDL, over a range of input test conditions. Since the correct output can be predicted by independent means, simulation is a powerful verification approach, however, simulation is, at best, "a compromise between breadth of coverage and resources—time and computer power" [72]. The extent of the compromise determines the level of confidence in the design.

Tools and methods are being developed to address the limitations of the simulation compromise in breadth of coverage, time, and computer resources; however, it seems that the tradeoff is unavoidable since, for example, the coverage tool described above adds time to the simulation as it tracks the simulation progress. Tools and methods that address simulation time typically resort to less detailed models or other abstractions that may compromise breadth of coverage. Methods that exploit hierarchy may offer the best tradeoff, where portions of the design are partitioned and verified independently at detailed levels and then abstracted to higher levels for systemwide verification.

Formal verification techniques attempt to provide certainty via proof rather than a level of confidence as is associated with simulation approaches. Formal verification techniques may provide a measure of design assurance; however, the level of assurance provided is only as good as the mathematical basis of the technique and validation of the formal verification technique remains an issue. In general, formal verification proves the correctness of the design. Three broad approaches are theorem proving, symbolic model checking, and functional equivalence checking. The size of the designs that can be verified using formal methods is limited by the exponential relationship between the number of inputs and the total state space of the system. The amount of computer resources that would be required for large systems is prohibitive. As might be expected, research is focused on techniques to reduce the number of latches that need to be considered during the verification [72].

Model and equivalency checking are considered enabling verification techniques being developed and used at International Business Machines (IBM) in their design methodology for the IBM PowerPC [72]. Recently, EDA vendors, such as Chrysalis, have introduced commercially available formal verification tools for equivalency checking and model checking. References 73 and 74 provide further discussion, a list of additional formal methods tool vendors, and mentions Cray Research as another user of these tools.

Formal equivalency and model checking may provide a powerful verification tool in the microelectronics design process because it may provide an independent means of verifying the outputs of other tools used in the design process. For example, synthesis tools may be used to generate transistor level implementations of the design from register transfer level (RTL) representations. The formal checking methods may provide an approach to verify that the two representations are equivalent.

Fault coverage tools provide the capability to identify the fault coverage afforded by a certain set of test vectors. The tool evaluates the design model and determines if faults such as stuck-at, open, and drive level will be evidenced at the outputs, as an output vector which is distinct from all the normal output vectors. It also identifies faults that are not evidenced by the set of test vectors under consideration [75].

Postlayout EDA tools are available which allow the extraction of parasitic parameters such as the resistance and capacitance of interconnects. For submicron designs, the interconnect time delay will dominate the dynamic timing of the circuit, and postlayout extraction tools allow verification of critical timing circuits. Reference 76 provides discussions and an extensive list of tool vendors.

A sampling of the latest EDA tools released at the June 1999 Design Automation Conference is provided in reference 77.

4. ISSUES WHICH LIMIT THE ABILITY OF COTS COMPONENTS TO MEET DO-254 OBJECTIVES.

The following Key Component Attributes were identified through review of DO-254 objectives:

- Design Assurance
- Component Reliability
- Standards
- Failure Modes
- Operation Beyond Mfg. Spec.
- Upsets
- Service Experience
- Configuration Management
- Production Practices
- Verification Testing
- Role of COTS Tools in Design and Verification

COTS components may have issues, relative to these key attributes, which limit their ability to meet DO-254 objectives. Some of these issues are identified in the following section.

4.1 DESIGN ASSURANCE.

Issue: "Actual availability of COTS component design assurance data as required by DO-254" (see section 11.2.2 of reference 1).

Hardware design assurance is intended to address the dilemma posed by all complex hardware relative to safety requirements. For complex electronic hardware, it is relatively straightforward to prove that the component meets the requirements of the intended function; however, it is very hard, if not impossible, to prove that the component will never exhibit anomalous behavior due to malfunction or unintended function. The role of design assurance is to provide a structured, disciplined design process that is commensurate with the risk of the associated safety function. The level A or B safety functions, implemented in complex components, require acceptable design assurance evidenced by design assurance data. Further description is provided by Rierson, Struck, and Beane in "Complex Electronic Hardware" IVT Course Number 62816, FAA, July 28, 1999, which can be found at http://av-info.faa.gov/software/cmplx_Hdwr/CEH guide.pdf.

"A hardware item is identified as simple only if a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior." "Items that contain a device, such as an ASIC or a PLD, can be considered simple if they meet the criteria" (see section 1.6 of reference 1). All criticality levels, A-E, which incorporate only simple components, do not require extensive design assurance because, by virtue of meeting the criteria for simple components, both intended and unintended functions can be completely assessed through deterministic verification methods and assured through configuration management methods.

The DO-254 Appendix C definition of COTS component is a "Component, integrated circuit or subsystem developed by a supplier for multiple customers, whose design and configuration is controlled by the supplier's or an industry specification." Clearly, supplier control of the design precludes the execution of a safety requirement-driven design assurance strategy during the design process. Detailed information regarding the design of COTS components may be considered proprietary by the commercial company and, if such information does exist, the company may refuse or be reluctant to release it.

4.2 COMPONENT RELIABILITY.

Issue: Actual availability of COTS component data as required to determine failure rates by an acceptable method.

Component reliability is concerned with assuring the derived hardware requirements with respect to failure rates are met. Failure rates can be determined by a number of methods, including analytic prediction methods, accelerated life testing, and service experience analysis. Each method requires some form of input data to carry out the method. Analytic prediction methods may require detailed design data. Accelerated life testing requires configuration controlled components, details of failure mechanisms to be addressed, and target operating environment. Service experience analysis requires high-quality field data relevant to the target application.

4.3 STANDARDS.

Issue: Standards for electronics development and production are diverse, do not address the needs of critical systems, and are no longer supported by the federal government.

4.4 FAILURE MODES.

Issue: It may be difficult to identify all fault modes, i.e., anomalous behavior, for complex COTS components.

Failure modes are the various ways by which a component may exhibit anomalous behavior. Anomalous behavior may be the result of an element that fails to perform its intended function such as a connection which opens or a transistor that fails to turn on. While component reliability is concerned with the rate of elemental failures within a component, fault mode identification and mitigation are fundamental to meeting safety requirements. DO-254 requires Functional Failure Path Analysis (FFPA) for level A and B functions, and suggests FFPA may also be of value for functions of lower criticality. The FFPA clearly requires the identification of failure modes which impact safety requirements and requires decomposition of the system to the extent necessary to meet requirements.

COTS components may exhibit failure modes as a result of element failure within, however, other sources of anomalous behavior may exist, such as unintended functions or parameter variation due to operating environment.

4.5 OPERATION BEYOND MANUFACTURER'S SPECIFICATION AND UPSETS.

Issue: COTS component suppliers discourage use of their components in unintended environments

Issue: The manufacturer-specified operating range of COTS components do not meet the requirements for many airborne applications

Issue: COTS components may exhibit anomalous behavior due to EMI and radiation.

COTS components are generally targeted at markets where the operating environment is benign with respect to many airborne applications. Ruggedized-off-the-shelf (ROTS) board-level products are available with extended operating ranges specifications; however, these products are specifically targeted at DoD applications as a niche market, and while they meet the DO-254 definition of COTS components, their customer base is currently almost exclusively DoD related. The airborne application operating environment presents challenges in the areas of temperature extremes, shock and vibration, humidity, and upsets including EMI and radiation. Extensive testing programs sponsored by both the government and OEMs are focused on determining the extended range capability of COTS components. The use of components beyond their manufacturer-specified range should be avoided if possible.

4.6 SERVICE EXPERIENCE.

Issue: The quality of COTS service experience data may be inadequate to meet safety requirements.

The widespread use of a COTS component by many users in multiple applications serves to surface component deficiencies that can then be corrected by the supplier. "Wide and successful

use of an item in service may provide confidence that the item's design is mature and free of errors and that the manufacturing quality of the item is demonstrated" (see section 11.3 of reference 1). DO-254 recognizes that service experience can be an important contributor to design assurance, quality assurance, and component reliability assessment; however, the service experience data must meet acceptance criteria for completeness and applicability to the system safety requirements. Warrantee repair/replacement data is the type of service experience data most likely to be documented by COTS suppliers, but it is of marginal value with respect to meeting safety requirements. At least limited service experience data can be obtained from other sources.

4.7 CONFIGURATION MANAGEMENT AND PRODUCTION PRACTICES.

Issue: COTS suppliers are at liberty to change their production processes.

Issue: COTS suppliers are at liberty to discontinue production of a component resulting in "COTS components which become non-procurable" (see section 11.2.2 of reference 1).

Issue: "Variations in component parameters that depend on production batches may not be identified, even by robustness tests" (see section 11.2.2 of reference 1).

Issue: "Evolving aspects of electronic component technology" (see section 11.2.2 of reference 1).

Issue: Quality control provided by COTS suppliers may be inadequate

Since the COTS component's "design and configuration is controlled by the supplier's or an industry specification" (see Appendix C of reference 1), configuration management and production practice issues are dependent on the COTS supplier performance as well as the OEM responsible for the performance of the system. Identifying appropriate COTS suppliers, establishing relationships and agreements, and continued supplier monitoring are essential aspects of the successful development program. However, since the COTS supplier is market driven, fallback approaches should also be developed to handle supplier problems.

The ideal incorporation of COTS components would be to employ the components as supplied to the commercial market; however, the needs of the safety critical system are significantly more demanding than the commercial market, creating issues where the needs of commercial and safety critical diverge.

4.8 VERIFICATION TESTING.

Issue: Production testing done by COTS suppliers may fail to detect defective components.

Issue: OEMs may not have sufficient design information or resources to adequately test complex components.

The extent of verification testing done by COTS component suppliers is typically determined by a tradeoff between the cost of testing, process yield, warrantee costs, and customer acceptance.

In some cases, OEMs negotiate with their suppliers to establish the best tradeoff to allow the OEM to meet safety requirements.

4.9 ROLE OF COTS TOOLS IN DESIGN AND VERIFICATION.

Issue: Design tools used by both COTS suppliers and OEMs may introduce design errors.

Issue: Verification tools used by both COTS suppliers and OEMs may fail to identify defective components.

Design and verification becomes more dependent on the use of tools as the complexity of the component increases. Commercial market pressures dictate rapid design development, increased functionality, and low-cost production. Tools, while lagging behind the technology, are evolving to meet the needs of the commercial market. Again, the needs of the safety critical system are significantly more demanding than the commercial market, creating issues where the needs of commercial and safety critical diverge.

4.10 SUMMARY OF IDENTIFIED ISSUE.

- Design Assurance

  Issue: "Actual availability of COTS component design assurance data as required by this document" (see section 11.2.2 of reference 1).

- Component Reliability

  Issue: Actual availability of COTS component data as required to determine failure rates by an acceptable method.

- Standards

  Issue: Standards for electronics development and production are diverse, do not address the needs of critical systems, and are no longer supported by the federal government.

- Failure Modes

  Issue: It may be difficult to identify all fault modes, i.e., anomalous behavior, for complex COTS components.

- Operation Beyond Manufacturer's Specification and Upsets

  Issue: COTS component suppliers discourage use of their components in unintended environments.

  Issue: The manufacturer-specified operating range of COTS components do not meet the requirements for many airborne applications.

Issue: COTS components may exhibit anomalous behavior due to EMI and radiation.

- Service Experience

  Issue: The quality of COTS service experience data may be inadequate to meet safety requirements.

- Configuration Management and Production Practices

  Issue: COTS suppliers are at liberty to change their production processes.

  Issue: COTS suppliers are at liberty to discontinue production of a component resulting in "COTS components which become non-procurable" (see section 11.2.2 of reference 1).

  Issue: "Variations in component parameters that depend on production batches may not be identified, even by robustness tests" (see section 11.2.2 of reference 1).

  Issue: "Evolving aspects of electronic component technology" (see section 11.2.2 of reference 1).

  Issue: Quality control provided by COTS suppliers may be inadequate.

- Verification Testing

  Issue: Production testing done by COTS suppliers may fail to detect defective components.

  Issue: OEMs may not have sufficient design information or resources to adequately test complex COTS components.

- Role of COTS Tools in Design and Verification.

  Issue: Design tools used by both COTS suppliers and OEMs may introduce design errors.

  Issue: Verification tools used by both COTS suppliers and OEMs may fail to identify defective components.

5. ALTERNATE METHODS TO MEET DO-254 OBJECTIVES WITH COTS HARDWARE (HW).

5.1 ADVANCED ELECTRONIC DESIGN AUTOMATION.

5.1.1 Electronic Design Automation Overview.

The complexity of ICs has rapidly increased, with state-of-the-art devices now containing over 40 million transistors. A single chip is now able to provide the circuitry that previously required

several ICs and associated printed circuit board interconnections. The increased complexity of ICs has enabled the development of a myriad of commercial products that provide new levels of function and performance. Computers, wireless communications, and internet hardware are enabling new information exchange, at an affordable cost, which is having revolutionary effects on almost every aspect of the economy.

The time to market for new products is critical to success in the current commercial environment. While the increased complexity of ICs enables high functionality, at low cost, the development time of advanced ICs increases the product development cycle time and thus jeopardizes product success through increased time to market. "EDA products play a critical role in reducing time-to-market for new products by providing IC designers with tools and techniques to:

a. reduce the time and manual effort required to design, analyze, and verify individual ICs,
b. improve the performance and density of complex IC designs and
c. enhance the reliability of the IC design and manufacturing process" [78].

The supply of IC designers with the skills and experience necessary to develop high-complexity ICs does not meet the demand. The use of advanced EDA tools is seen, by some, as an approach to increased productivity for skilled designers, but also as a means to supplement the capabilities those who are less skilled. If less skilled designers are relying on EDA tools to automate portions of the development cycle, it will become critical that the capabilities and limitations of the design tools be understood to avoid misuse and potential design flaws.

After delivery of the first engineering prototypes of a complex IC, the time required for debug and redesign may account for 40% to 45% of the development time [79]. Problems encountered include functional, timing, power consumption, and high-current densities, causing early failure through electromigration. Identification and analysis of prototype problems consume engineering resources, increase development time, and can result in redesign and production of corrected prototypes. While complex ICs reduce unit cost by packing more functionality into smaller die sizes, the development costs must be controlled by using design methods that result in a successful prototype on the first attempt.

Young suggests the following items are essential to successful design:

- Mature, production-proven analysis and verification tools and methodologies confirm function, timing, power, etc. These tools must have "algorithm quality" to support the performance, precision, and capacity requirements of nanometer designs.

- Silicon-calibrated layout parasitic and device extraction enable viable verification. The accuracy of the best analysis and verification tools is only as good as the layout data extracted and annotated.

- Reliability analysis is required to ensure the design is production-ready and volume-worthy. Issues of robustness and reliability can prevent first-pass silicon from working to specification. Designers need tools and methodologies to verify that the complex power

distribution systems present on today's ICs are robust enough to control IR drop and to support current densities beneath that at which electromigration becomes an issue [79].

Design challenges are being faced in many areas, including timing analysis, power consumption, cross-talk, metal migration and power distribution, within the IC. Railmill, a product by Synopsys, is claimed to hold 95% of the EDA reliability analysis and verification market, and Synopsys is investing over 150 million dollars a year in research and development. New EDA tool developments will allow designers to address the design challenges earlier in the design process, providing additional design assurance which was previously unattainable.

5.1.2 Timing Analysis.

Small transistors and single chip proximity have allowed complex ICs to achieve GHz performance. However, timing analysis for complex ICs has become more challenging, since the standard design rules once used for larger transistors ICs are no longer adequate. At smaller chip scaling, the delay times associated with interconnections have significant impact on dynamic performance. New generation design tools feed physical design layout geometry back into the logic design process to account for the resistance, inductance, and capacitance of the interconnects and provide more accurate timing estimates. These tools iterate between synthesis and the physical design, i.e., placement and routing of the gates, to assure the physical design meets timing requirements.

5.1.3 Power Supply Network.

The power supply network within complex ICs poses new design challenges as metal lines become smaller and transistor currents become higher due to higher clock frequencies and lower transistor on resistance. Previous design methods assumed constant supply voltages at the transistors regardless of the currents being switched. As feature sizes get smaller, this assumption is not longer valid. The designer can compensate by over designing the power distribution network or use accelerated testing of prototypes to expose design problems. EDA tools that evaluate the IR drop throughout the power distribution network presents a third option to provide design assurance.

5.1.4 Electromigration (EM).

EM is an effect that gradually degrades metal interconnects, contributing to wear out of the IC, i.e., limiting the useful lifetime. In complex ICs, high-current densities, resulting from reduced geometry, combine with high temperatures, resulting from high-power density, to produce EM effects were previously not significant. EDA tools, which address EM verification, may provide design assurance that EM effects will not cause premature IC failure. The ability to predict EM effects during design may also allow designers to tradeoff lifetime for additional functionality, resulting in lifetime goals of, say, 5 years for markets where products rapidly become obsolete.

5.1.5 Unifying Language.

Design development for complex ICs currently uses a hardware description language such as Verilog or VHDL. However, for complex ICs, a programming language like C/C++ is often

used for simulations of portions of the system using behavioral models. Some see the need for a new unified language, which can both describe hardware and extend the capabilities of C/C++ into the hardware domain [80].

The Open SystemC Initiative, supported by Synopsys, Coware, Lucent Technologies, and Texas Instruments, hopes to establish SystemC as the de facto standard. Superlog is an alternative language being developed by Co-Design Automation Inc. The goal is to have a standard language in which "semiconductor vendors, intellectual property (IP) vendors, and system houses could exchange system-level IP and executable specifications, and the electronic design automation industry could develop interoperable tools" [80].

Currently, EDA tools must support both Verilog and VHDL. In addition, interface between EDA tools is an industrywide problem. The adoption of one of the emerging new languages may eliminate obstacles which currently exist with respect to information exchange during in IC design.

5.1.6 Emulation.

Emulation is a design verification method that translates the IC design into FPGAs. Functional performance can be evaluated using FPGAs, prior to producing silicon prototypes. Typical emulation platforms provide a few MHz of performance which makes verification of thousands of operations very time consuming. New high-end FPGAs, with one million gates each, operating at 100 MHz, are providing high-performance emulation platforms as needed for complex ICs.

5.1.7 Simulation.

Simulation verifies correct operation of the design by applying test vectors and comparing the design response to expected outcomes. For complex ICs, the number of test vectors required to fully verify a design makes simulation verification very time consuming.

5.1.8 Model Checking.

Model checking is a form of formal verification that attempts to prove the properties of the synthesized design are the same as those of the higher level of abstraction model. For designers who are familiar with simulation and static timing methods, model checking methods present a very different approach to verification. The complexity of the circuits, which can be model checked, while expanding, is limited. Model checking cannot handle some types of circuits, such as multipliers [80].

5.1.9 Crosstalk.

Crosstalk between signals becomes more significant as line spacing between interconnects drops into the submicron spacing. The physical design should be verified for this type of signal integrity before producing prototype silicon, in order to avoid the redesign, which may be required if crosstalk problems are discovered in the silicon.

5.2 APPROACHES TO MITIGATE UNDECLARED, UNUSED ADDITIONAL FUNCTIONS (UUAF).

DO-254 raises justified concerns with respect to the impact of undeclared, unused additional functions on safety, since they may result in unidentified anomalous behavior. Detailed design data, if available, may allow the effects of UUAF to be adequately identified for FFPA purposes. No alternative methods with respect to UUAF were discovered during the course of this investigation.

5.3 COMPONENT RELIABILITY.

5.3.1 Empirical Models for Reliability Prediction.

Empirical models for device reliability are developed based on both laboratory test data and filed data. Failure analysis data is analyzed to find a statistical correlation between mean time to failure (MTTF) and the electrical and operating stress factors believed to contribute to the failure mechanisms. The correlation models are then used to extrapolate the failure rate of the devices under operating conditions of the intended application. Steady-state temperature and relative humidity are typical factors that are correlated to corrosion and other degradation effects to predict device MTTF. Statistical techniques are used to develop model parameters through curve fitting to the available data.

The failure rate of a device is assumed to be constant over its operating lifetime, after the infant mortality phase, which is assumed to be eliminated by burn-in of the devices.

Failure rates for systems are determined by summation of the failure rates for components comprising the system.

For a particular device, the failure rate prediction may be a weighted average of field data and industry standard data, with weighting of field data dependant on the amount of field data available. The accuracy and quality of the field data should also be taken into consideration.

Handbooks provide guidance in failure rate prediction based on empirical methods. The following examples of prediction handbooks is provided by [81]:

- Bellcore Handbook TR-TSY-000332;
- British Telecom Handbook;
- Centre National D'Etudes des Telecommunications (CNET) Handbook;
- IEC 56 Sec 60348;
- MIL-HDBK-217;
- Nippon Telegraph and Telephone Handbook;
- RAC-EPRD;
- RAC-VZAP;
- Siemens Standard SN29500; and
- SAE 870050

The International Electrotechnical Commission (IEC) cautions that handbook predictions are not recommended. If they are employed, it is important to select the proper handbook for the targeted equipment. Handbook data may be supplemented or replaced by the user if data more appropriate to the application is available and justified.

The NavSea Naval Sea Systems Command specifies that "The Reliability Prediction of Electronic Equipment Handbook, MIL-HDBK-217F notice 2, is used as a guideline to establish and maintain probability for microcircuits" [82]. However, NavSea provides an example of users who chose to modify 217F data. The quality factor for consumer plastic-encapsulated microcircuits is being reduced from 10 to 4 and the environmental factor is 0.5 for protected environment and 5.0 for the normal environment [82].

Empirically based reliability prediction methods, and in particular MIL-HDBK-217, have been criticized for the following shortcomings identified in reference 44:

- Method is not a good indicator of field reliability
- Temperature cycling is not accounted for
- Method does not reflect new manufacturing trends
- Method does not differentiate good quality and design practices
- System level factors that influence reliability are penalized (e.g., transient protection circuits)
- Method is not science based

5.3.2 Similarity Analysis.

Similarity analysis is based on field, test, or operational failure data for a predecessor product that exhibits both similarities and differences with respect to the product to be evaluated. The rate of failure is determined as a composite of all root causes for the product. The analysis should include methods to quantify similarities and differences between the predecessor and the product being assessed. The reliability of the known product is adjusted based on similarities and differences to predict the reliability of the new product [81].

Reference 81 suggests the following elements for comparison, in appropriate level of detail:

1. Operating and environmental conditions (measured and specified);
2. Design features;
3. Design processes;
4. Reliability assurance processes;
5. Manufacturing processes;
6. Maintenance processes; and
7. Components and materials.

Note that design processes used in the predecessor product are elements of comparison that may be difficult to assess for COTS components.

Predecessor product data must be analyzed to determine a model for the field return behavior. Statistical distributions and polynomial curve fitting may be used to analyze return data, population data, time in field, and time to return. Confidence levels should be used to bound the reliability prediction of both the predecessor and the product being assessed. Clearly, the quality of the predecessor data impacts the confidence of the reliability prediction.

A method called Failure Cause Modeling is described in reference 81. The method is used when no single predecessor product is sufficiently similar to allow similarity analysis. In Failure Cause Modeling, a number of different predecessor product assessments are considered, using the comparison elements of similarity analysis. By using elements of previously performed similarity analysis, an end item failure model is constructed.

5.3.3 Physics of Failure.

Reference 81 describes a durability assessment method that incorporates physics of failure techniques as follows:

- Determine operational and environmental stresses that the equipment will experience throughout its life, including shipping, handling, storage, operation, and maintenance.
- Determine sites where failures are likely to occur using, for example, FMEA.
- Determine the magnitudes and locations of significant stresses using, for example, FEA.
- Determine how long the significant stresses can be withstood or sustained using the appropriate damage models, e.g., Arrhenius equations, inverse power laws, etc.
- Report the results as a list of failure sites, mechanisms, and modes; rank-ordered according to the time expected for failure to occur.

Damage models for failure modes relate the level of a particular form of stress to the time that the component can withstand the stress before failure. These effects are typically associated with the device wear-out phase of the traditional "bath tub" reliability curve.

Numerous failure mechanisms must be considered, including "electro-migration, solder joint cracking, die bond adhesion strength, die cracking, bond wire corrosion, etc." [44]. Component failure models for these and other failure mechanisms can be found in the literature, such as IEEE International Reliability Physics Symposium Proceedings, the Holm Conference Proceedings, several publications of the IEEE Components, Packaging and Manufacturing Technology Society, and the IEEE Electron Devices Society [41]. Model parameters are determined through detailed knowledge of the device, including device material characteristics and geometry.

Note that "MIL-STD-217 component failure rates are in large part based on use of a physics-of-failure model, Arrhenius rate. The argument about the Standard are focused on the fact that this may not be a very satisfactory model for many failure rates" [41].

Accelerated testing is targeted at precipitating failures quickly, by subjecting the part to stress levels which are elevated with respect to those that the device will see in normal operation. The lifetime of the test device is related to that of the field unit by a factor. Physics-of-failure models should be used to understand which stresses contribute to failure mechanisms and what valid conclusions can be drawn from the results of accelerated testing. An example of accelerated testing might be thermal cycling of a surface mount component to assess board attachment integrity. While accelerated testing can provide some assurances with respect to component robustness, this type of testing does not improve the ability to predict failure rates [41].

Physics-of-failure methods do not, in general, address the nature of random failures associated with the center, useful life, portion of the bath tub reliability curve where failures are due to defects, variable tolerances of components, and field conditions. Monte Carlo techniques could, however, be employed with respect to part tolerances, to build a stochastic representation from the deterministic models [41].

"Physics-of-failure methods predict when a single specific failure mechanism will occur for an individual component due to wear-out (end of life)" [44]. A component may have numerous failure mechanisms, and the model for each requires component specific, detailed knowledge of geometry and materials. "A physics-of-failure type of analysis is most beneficial at the device level where the device design can be influenced, such as with newly developed hybrid circuits, or in investigating an established problem" [44].

Reference 44 provides the following recommendations for appropriate use of empirical and physics-of-failure methods.

- Use Empirical Methods:
  - When reliability estimates are performed for large, complex products
  - When reliability estimates are developed on a quick-turnaround basis
  - When there is a need to estimate the relative merits of competing designs
  - When there is no way to change the fundamental design of the components
  - When the only design flexibility is to select different components or limit applied component stresses
- Use Physics-of-Failure Methods:
  - When a detailed understanding of life-limiting failure mechanisms is needed

- When new component technologies need to be assessed and no historical data exists
- For detailed component design prior to life testing and qualification
- When design flexibility exists at the component level
- To investigate the root cause of a failure

Physics-of-failure models are the basis of handbook predictions and design rules used in EDA tools for IC silicon layout. Electron migration, as previously discussed, is an example of a wear-out type failure mechanism, which physics of failure predicts, based on chip geometry. For submicron geometries, in commercial applications, the designer can tradeoff useful lifetime for added functionality, resulting in failure due to wear-out mechanisms after, say 5 years, instead of the traditional goal of 10 to 15 years. For commercial applications a 5-year lifetime may be more than adequate in some markets. Knowledge of the design rules and target lifetime for COTS components may soon become an issue in safety critical applications.

5.3.4 Field Data Analysis.

Field data analysis identifies the true reliability performance of the product and verifies (or not) the reliability predictions made in early stages of design. Reliability in actual field usage can be used to formulate corrective action for the product and provide feedback to the development of future products.

A failure may include both true failures, where the product failed to perform properly, and returns, for which the cause of return is unknown and may not be due to a true failure. Improper application, poor quality assurances, or poor troubleshooting techniques may contribute to returns. The result of a field data analysis will be of value for some reliability metrics such as MTBF or failures per 1000 hrs.

Field data is needed in each of two categories: installed base quantity and failure quantity per unit time. The quality of the installed base should give the most accurate representation of the number of units in actual field use. The failure quantity should correlate with the quantity of installed base. Additional detailed product information, such as product type, site of manufacture, configuration, and options can be used, if available, to get a reliability measure for a more specific product type or usage. It is often beneficial to obtain information that will allow the calculation of the age of the unit at the time of failure.

Failure distribution is critical to understanding the reliability of a component. Since "identical" components are expected to fail at different times, failure phenomena should be described in probabilistic terms. The selection of the distribution should be based on specific knowledge of the failure physics at work, or at least some previous experience with a similar product. An exponential distribution is often used to describe the failure of electronic components in the useful life or flat portion of the bath tub curve; however, "many times one is forced to select a distribution model without having sufficient data to verify its validity" [41].

5.3.5 PRISM Reliability Assessment Methodology.

PRISM is a software tool for estimating the failure rate of electronics systems based on a new methodology developed by the Reliability Analysis Center (RAC). Both component reliability prediction models and methods to assess the impact of noncomponent variables on system reliability are provided. RAC developed the system assessment methodology to overcome some of the perceived limitations of MIL-HDBK-217. The work is based on an Air Force study performed by RAC and Performance Technology.

Reference 43 provides a description of the new PRISM methodology which makes use of new "RACRate" models, additive reliability models rather than the traditional multiplicative approach, and grading factors for a number of processes identified as having impact reliability such as manufacturing. The following provides excerpts from reference 43, description of the methodology:

> *"The purpose of PRISM is to provide an engineering tool to assess the reliability of electronic systems. It is not intended to be the "standard" prediction methodology, and it can be misused if applied carelessly. It does not consider the effect of redundancy or perform FMEAs. The intent of PRISM is to provide the data necessary to feed these analyses. The methodology allows modifying abase reliability estimate with process grading factors for the following failure causes: parts, design, manufacturing, system management, wear out, induced, and no defect found. These process grades correspond to the degree to which actions have been taken to mitigate the occurrence of system failure due to these failure categories. Once the base estimate is modified with the process grades, there liability estimate is further modified by empirical data taken throughout system development and testing. This modification is accomplished using Bayesian techniques which apply the appropriate weights for the different data elements. Advantages of this new methodology are that it uses all available information to form the best estimate of field reliability, is tailorable, has quantifiable confidence bounds, and has sensitivity to the predominant system reliability drivers. The new model adopts a broader scope to predicting reliability. It factors in all available reliability data as it becomes available on the program. It thus integrates test and analysis data, which provides a better prediction foundation and a means of estimating variances from different reliability measures.*
>
> *An initial estimate of the failure rate is based on a combination of the new "RACRate" failure rate models developed by RAC, the empirical field failure rate data contained in the RAC databases, or user-defined failure rates entered directly by the user. This initial failure rate represents a "typical" system and "average" processes. It is then adjusted in accordance with the process grading factors, infant mortality characteristics, reliability growth characteristics, and environmental stresses.*
>
> *An objective of the PRISM system model is to explicitly account for the factors contributing to the variability in traditional reliability prediction approaches. This is accomplished by grading the process for each of the failure cause categories.*

The resulting grade for each cause corresponds to the level to which an organization has taken the action necessary to mitigate the occurrence of failures of that cause. This grading is accomplished by assessing the processes in a self audit. Any or all failure causes can be assessed and graded.

The PRISM model also includes a factor for assessing the reliability growth characteristics of a system. The premise of the factor is that the processes that contribute to system reliability growth in the field may or may not exist.

Infant mortality is accounted for in the model with a time variant factor that is a function of the level to which Environmental Screening Strength (ESS) (MIL-HDBK 344) has been applied.

Traditional methods of reliability prediction model development have included the statistical analysis of empirical failure rate data. The statistical methods typically result in a model form that is multiplicative (i.e., the predicted failure rate is the product of a base failure rate and several factors that account for the stresses and component variables that influence reliability). A primary disadvantage of the multiplicative model form is that the predicted failure rate value can become unrealistically large or small under extreme value conditions (i.e., when all factors are at their lowest or highest values). This is an inherent limitation of multiplicative models, primarily due to the fact that individual failure mechanisms, or classes of failure mechanisms, are not explicitly accounted for. The RAC believes that a better approach is an additive model which predicts a separate failure rate for each generic class of failure mechanisms. Each of these failure rate terms is then accelerated by the appropriate stress or component characteristic.

There are two primary types of data on which the "RACRate" models are based; failure rate and failure mode. The model development process requires that the failure rate data be apportioned into failure cause categories. Since the failure mode data contained in the RAC databases is typically not in these categories, it was necessary to transform the failure mode distribution data into the failure cause distribution. This was accomplished by assessing the stresses that accelerate the specific class of failure categories and estimating the percentage of failures that could be attributed to those stresses. The primary stresses that potentially accelerate operational failure modes are operating temperature, vibration, current and voltage. The stresses that accelerate environmental failure causes are non-operating ambient temperature, corrosive stresses (contaminants/ heat/humidity), aging stresses (time), and humidity. This data was collected by the RAC and is based primarily on failure analysis of parts that have failed in the field.

The user is encouraged to collect as much empirical data as possible and use it in the assessment. This is done by combining the assessment made (based on the initial assessment and the process grades) with empirical data. If test data is

available that was taken at accelerated conditions, it needs to be converted to the conditions of interest."

5.3.6 Reliability Model Assessment.

Reference 83 discusses criteria for determining if reliability models are actually valid.

In applications requiring high reliability and safety, the validity of reliability models used in the FFPA analysis should be established. The authors propose criteria for the assessment of reliability models that focuses on the three areas which impact reliability: environmental stress, design parameters, and manufacturing process.

Environmental loads traditionally include steady-state temperature and humidity, but should also include other effects such as temperature cycling, humidity cycling, power cycling, voltage bias, vibration, and radiation.

Detailed models should account for the relationship between the load and the intensity of the stress, which results at the failure site. For example, corrosion, which may be the dominant failure mechanism for plastic-encapsulated modules (PEMs), has been shown to be related to the water content inside the package. Water content may be empirically modeled as a function of ambient relative humidity through the material properties of the package encapsulate, thus accounting for the variations presented by the more than 400 different encapsulate materials in use.

Design parameters include the effects of materials and geometry, which have been shown to be significant, especially as complex IC geometry drops to submicron scales.

Manufacturing processes can significantly impact reliability.

Failure analysis should address three things: mechanism that causes the failure, the mode or observed effect of the failure, and the site or location of the failure.

Model distributions, which are traditionally employed, assume exponential or log-normal distributions, sometimes without adequate verification.

Activation energy concepts, in some cases, have been contradicted by empirical data.

Acceleration testing assumes that a failure mechanism active at higher stress conditions will also be active under normal operating conditions; however, studies have shown this is not always the case. In addition, the dominant failure mechanism may shift throughout the device's lifetime.

The author examines 12 common microcircuit reliability models and identifies the shortcomings of each with respect to the issues raised above.

The limitations of reliability models should be considered when using them for reliability prediction methods. Physics-of-failure model development is targeted at addressing model

shortcomings identified; however, detailed design information is clearly required to assess the mechanisms at this level of detail.

5.3.7 Activation Energy-Based Testing Assumptions.

Reference 84 provides a discussion on activation energy and test assumptions. Activation energy is shown to increase with time from 0.6 eV in 1975 to 1.0 eV in 1995. The trend is perhaps due to process quality improvements, which shrink the weak population with lower activation energy, there by increasing the activation energy of the population. This may mean that accelerated testing times, which are based on activation energy concepts, need to be re-examined. Shorter qualification tests may be possible because of increased acceleration factors associated with higher activation energy levels. For example, for a device of activation levels exhibited in 1985, 1 hour of testing at 150°C is treated as equivalent to 492 hours at 55°C; however, for a 1995 device, only 29 hours of testing at 150°C is required for the same 492 hours at 55°C operation. Longer life test time is required to get failure statistics for newer devices: 1995 device is 74× longer than a 1985 device. Testing for any unknown low-activation energy mechanism will still require long test times or high-stress levels [84].

5.4 FAILURE MODES.

The Reliability Analysis Center has identified eight predominate failure causes based on data collected during their activities.

- Part failure to perform its intended function. Part reliability is the focus of most reliability work as described in preceding sections.

- Design errors are the second predominate failure cause and is the focus of design assurances recommended in DO-254.

- Manufacturing process-induced errors.

- System management-induced failures due to improper interpretation of system requirements or inadequate delegation of resources required in design or fabrication of the product. DO-254 processes are requirement based.

- Wear out related failure mechanisms such as traditional problems with electrolytic capacitors or relay contacts. Useful life expectancy for complex ICs may become a wear-out issue as designers tradeoff lifetime mechanisms for added functionality.

- No defect failures are perceived failures that cannot be duplicated through further testing. Faulty connectors often result in no defect failures, attributed to a Lowest Replacement Unit (LRU), since replacement of the LRU reseats connectors, the problem appears to be solved by the new LRU.

- Induced failures result from external application of an exceptional stress, such as over voltage; or operational stresses, such as temperature or humidity.

- Software faults which result in the component not performing its intended function. DO-178B addresses software development for safety critical systems.

Many of these predominate failure causes identified by RAC are addressed by DO-254 and are the source of issues previously identified for COTS components.

5.5 OPERATION BEYOND MANUFACTURER'S SPECIFICATIONS.

5.5.1 International Electrotechnical Commission (IEC) Guidelines.

The IEC has produced a guidance document for the qualification of components for operation beyond the manufacturer's specified temperature range [85]. The practice is specifically discouraged, but it is recognized that in some cases there is no alternative. In no case should the component be operated beyond the component's maximum junction temperature with a 20°C margin.

"The technology of the component and its package should be identified and understood in sufficient detail to assess the likelihood and consequences of potential failure mechanisms" [85].

Component qualification test data should be analyzed to assure the package material is suitable for operation over wider temperature ranges, including higher mechanical stress levels and changes in material properties.

Component recharacterization guidance is provided. All electrical parameters which are critical to the application should be identified, recharacterized, and the recharacterized parameters evaluated with respect to application requirements. Interdependence of parameters should be considered. Sample sizes should be large enough to assure that normal variations have been accounted for in the recharacterization. The number of recharacterization temperature test points and the interval between test points require careful consideration and may be different for certain parameters.

"New and/or accelerated failure mechanisms, which might be evident at the wider temperature range, should be clearly identified and their effects on reliability established" [85].

Testing at higher assembly levels should be conducted to assure uprated components perform their intended functions.

5.5.2 Component Stress Balancing Method.

"Component stress balancing consists of operating the component at a temperature above that specified by the component manufacturer; and compensating by reducing at least one of the other operating parameters, e.g., power, speed, to the extent that the junction temperature remains below its maximum rating, with acceptable specified margin" [85].

Reference 86 provides an example of the method as applied to a CMOS octal tristate buffer chip rated for operation from -40° to 85°C ambient temperature. The application required the chip to operate in a -40° to 100°C temperature environment. Power dissipation is analyzed to determine

that if the power dissipation is kept below 170 mW, the junction temperatures for the chip will be below the manufacturer's specifications. Reduced operating voltage was ruled out as a stress balancing opportunity due to interfacing requirements. The IC was rated for 13-MHz operation at 25°C ambient temperature. By limiting the frequency of operation below 6 MHz, it was determined that operation at 100°C ambient temperature could be achieved. Further reduction of the operating frequency would allow operation at higher temperatures as long as the technique provided junction temperature at safe levels.

Detailed information is required to properly analyze the power dissipation and determine operating junction temperatures. For complex ICs, hot spots in the die should be identified with the help of the manufacturer. The power dissipation is not the output power, but rather that which is dissipated as heat. Depending on the information available through data sheets, intermediate power calculations may be required. The method is only useful for operation above the manufacturer's specified temperature, not below.

5.5.3 Cocooning.

Cocooning is an approach which regulates the environment seen by the component, such that the manufacturer's specified environment is maintained. One or all of the following provisions may be required:

- A regulated power source
- Regulated temperature
- Shock mounting
- Vibration isolation
- Humidity regulation
- Electrical shielding
- Contaminate protection

Cocooning has been used successfully in military applications of COTS components, especially board level components; however, the cost of the cocooning provisions can be significant.

5.6 UPSETS.

Component upsets may be caused by random occurrence of radiation or EMI. Airborne and space applications are effected by upsets, which are not generally experienced by commercial applications. While QML and other component suppliers provide radiation-hardened components, these devises are specially designed and tested for the environment. Government-sponsored device characterization programs are the primary source of advancement in this area. No alternative methods with respect to upsets and COTS components were discovered during the course of this investigation.

5.7 CONFIGURATION MANAGEMENT.

5.7.1 Mitigating Parts Obsolescence.

Parts obsolescence is a significant problem for military and airborne applications that require equipment lifetimes of 20 years or more. Commercial components are becoming obsolete after several years, with an Intel Memory Management Controller (MMC) chip reported to be in production for only 18 months. While 30 years ago the military applications accounted for 10% of the semiconductor market, in 2000 the military sector dropped to 0.03%, while computers and communications sectors rose to 57% and 17% respectively [87].

The Semiconductor Industry Association's Government Procurement Committee (SIA/GPC) formulated the following recommendations to minimize the effects of parts obsolescence [87].

- Purchase Defense Supply Center, Columbus (DSCC) standard microcircuit drawing products from Quality Manufacturers List (QML) suppliers to increase demand, enhance lifetime, assure quality and reliability.
- If commercial grade or industrial grade parts are selected, make no special changes and do not request special handling procedures or upgrade screens that make them low volume, source-controlled drawing ICs with questionable life times.
- Contracting changes and reforms are needed.
- OEMs and semiconductor suppliers must team to select components which will meet the required lifetime.
- DoD and OEMs must address Diminishing Manufacturing Source (DMS) from a broader perspective, not program by program.
- Contract funding should be allocated to address the problem.
- Utilize after-market suppliers, integrated with a semiconductor support plan.

The IEC has identified the following approaches to mitigate parts obsolescence [85]:

- Manufacturer negotiation
- Lifetime buy
- Substitute part
- After-market source
- Emulation
- Redesign
- Reclaim
- Reverse engineer

5.7.2 Technology Insertion.

Technology insertion is an approach suggested for military applications. Equipment which is designed for technology insertion employs open architecture and functional partitioning to allow technology upgrade through circuit board substitution. Open System Core Avionics Requirement (OSCAR) is an example of a military program structured to allow insertion of new single board computers as required for technology upgrade and mitigation of parts obsolescence. OSCAR is supported by Boeing and General Dynamics Information Systems and used on the AV-8B jump jet, the F-15 fighter, and the F/A-18 fighter-bomber. Technology insertion requires part change assessment and other assurances described in DO-254 and must be supported by development work throughout the life of the product.

5.7.3 Wafer Banking.

Wafer banking is an approach similar to lifetime buy. A number of completed wafers are procured and placed in inventory to assure a supply of die for subsequent component production. Wafer-banking inventory is less expensive then that of completed ICs, especially if the components remain unused. (After-market sources often wafer bank after original manufactures discontinue production in speculation of future sales at premium prices.)

Parts obsolescence will persist as a problem for OEMs serving markets that require supported lifetimes of 20 years or more. Commercial market trends will make parts obsolescence even more significant in the future. Alternate methods currently employed to mitigate parts obsolescence are all very costly. It remains to be seen, if the current COTS trend in military programs can be supported at reasonable cost over the life of the systems.

5.8 VERIFICATION TESTING: PRODUCTION TESTING TECHNIQUES.

The following story, related in reference 88, helps provide perspective for the importance of commercial device testing:

> *"Imagine yourself at the center of this scenario: Customers begin complaining about alarming failure rates in an assembly your company supplies. The quality-assurance department traces the failures to an ASIC that you helped to design; many of the devices fail after only 6 months. You visit the ASIC foundry and confirm that the personnel are faithfully following your device-test procedures; the procedures just don't catch the process-related flaw that triggers the failures. Manufacturing must scrap or rework 1.2 million assemblies that contain the defective IC, but the company has shipped and must recall 400,000 of those assemblies. The problem reduces the company's shipments for the quarter by $170 million and net profits by $37.7 million. Wall Street analysts downgrade the stock and question whether the company can survive.*
>
> *A fictional nightmare? Hardly. Events similar to these unfolded last summer at a major hard-disk manufacturer, at the foundry that makes the motor-control ASICs, and at the many PC manufacturers that buy the drives. The situation*

affected even the end users. By the time PC vendors recognized the problem, PCs containing the defective drives had apparently reached distribution."

This story clearly identifies the motivation for commercial component developers to assure the quality of their products and also the fact that flawed components sometimes make it into fielded systems. Despite the fact that commercial suppliers are motivated by the financial ramifications of design and verification errors, new developments to address the problem in the commercial industry may serve to provide methods of increased design assurance relative to safety requirement driven systems.

Dramatic improvements in manufacturing quality have been realized over the past 10 years, especially in high volume production lines with extensive process controls in place. At the same time, the cost of test for complex ICs has risen to nearly half the manufacturing cost. "The problem has become so severe that some in the IC industry have seriously contemplated doing away with testing. Their rationale: Quality is high; let the customers find the few defective parts" [88]. Commercial components which are used in low-cost entertainment products, like CD players, represent the market extreme where such a tradeoff may be seriously contemplated. Clearly, it is totally unacceptable for the needs of airborne systems, and in most commercial products, test is essential. For complex ICs, tests must become an integral part of the design process, and this will require the emerging cooperation of several groups including IC makers, EDA tool suppliers, Automated Test Equipment (ATE) suppliers, and suppliers of Intellectual Property (IP) such as built-in self-test (BIST) circuits.

In the commercial market, managers are now recognizing the importance of quality, and rewarding designers for the design of testable, defect free products as well as the meeting of compressed project schedules [88]. Designers need large amounts of quantitative data for prototype characterization, however, manufacturing test requirements must achieve a cost-effective balance between two outcomes which both lead to lost revenue: defective devices which the test process characterizes as good and good devices which the test process miss-classifies as defective.

Testing of complex ICs will require the use of several test methods. BIST will be cost-effective for structural testing, while ATE will be utilized for functional testing.

5.8.1 Built-In Self-Test (BIST) and Structural Testing.

As the operating frequencies of ICs increase, timing delays and uncertainties in test equipment become significant, relative to normal device variations. Test errors may be interpreted as device malfunction, resulting in rejection of good devices and lost revenue. On-chip test circuits are much closer to the elements under test than external circuitry, and high-frequency accuracy may be improved due to the shorter distances.

Boundary scan test instruments used in association with built-in self-test are relatively low cost. "New BIST techniques greatly simplify localization of the fault(s) in devices that exhibit problems [88]. Test vectors may be run at higher speeds then vectors associated with external ATE testers.

BIST is generally used to perform structural testing which attempts to verify that the device elements function according to the silicon design without defect in transistors or interconnects. Structural testing assumes that the silicon design will properly implement the intended function, therefore, if the device elements properly execute the silicon design, then the intended functions will operate properly.

Some argue that "because designers never have enough information to call most complex designs correct, they can't construct proper structural tests" [88]. In order to minimize test development time and vector sets which minimize test time, random vector sets may be used for logic tests. The use of random vector sets may fail devices for faults which are benign, relative to the function of the IC, but more importantly, random vector sets are most effective in detecting "stuck at" logic faults where a gate output is "stuck" in the one or zero state. While stuck at faults represented the majority of faults in older IC fabrication processes, in newer submicron designs, excessive propagation delays and interconnect bridging faults may be as prevalent as stuck at faults. Detection of delay and bridging faults present a challenge to test development for complex ICs and is the subject of ongoing research.

5.8.2 Automatic Test Equipment and Functional Testing.

Most ATE is used to implement functional testing, which attempts to verify that the device will perform its intended function. Functional testing is preferred for analog and mixed signal ICs. While functional testing typically employs fewer test vectors then structural testing, the issue of adequate test coverage remains a challenge which is of particular importance to safety critical applications. "Nobody seriously believes that a 50 mSec. test of a 2 million-gate ASIC can check every important operational condition" [88].

5.8.3 Virtual Test Software.

Virtual test software, developed by ATE and EDA suppliers, allows the designer to test simulated devices on simulated testers. This allows preliminary development and debug of the testing program to be done prior to receiving first silicon prototypes. Design for test techniques can be verified prior to commitment to first silicon, thus moving the test design effort earlier into the design development. Models currently available are imperfect, especially for analog and mixed signal ICs, so final debug must still be done on prototype devices; however, the use of virtual test software is claimed to reduce IC development by 6-8 weeks [88] and may provide additional design assurance.

5.8.4 Environmental Testing Approaches.

No alternative methods with respect to environmental testing approaches were discovered during the course of this investigation.

5.9 ROLE OF COTS TOOLS IN DESIGN AND VERIFICATION.

As the complexity of commercial electronic components increases, the design, verification of design, and production testing are becoming increasingly dependant on EDA tools. In addition, commercial pressures dictate that the layout of the chip be free of design errors on the first

attempt. EDA tools are evolving to meet the need for design verification during the design process. New tools are addressing sources of design errors which were previously only discovered during evaluation of the silicon. Despite increases in complexity, the coverage provided by these tools continues to improve.

COTS tools are fundamental in the design and verification of complex COTS components. EDA tools are being qualified, to some extent, by each design project. For example, if a chip exhibits timing problems, then the tools associated with the timing design verification obviously failed to provide the proper verification. While no industry survey of tool defects was discovered in this investigation, the tool supplier or user group publications may be a source of problem report information. It is recommended that such problem report mechanisms should be in place for tools used in airborne applications. Examples of successful tool usage in commercial applications are, of course, readily available from the tool supplier.

6. BARRIERS WHICH LIMIT THE ABILITY OF COTS COMPONENTS TO MEET DO-254 OBJECTIVES.

Each of the issues, identified as limiting the ability of COTS components to meet DO-254 objectives, presents significant challenges to the OEMs seeking benefit from the use of complex COTS components. The circumstances of COTS usage will be unique for each application, including the safety requirements which must be met, the system architecture developed by the OEM, the level of effort expended by the OEM in COTS component evaluation, and the cooperative efforts extended by the COTS supplier to the development effort. The use of COTS components in safety critical applications is simply not the type of application intended by the supplier. In fact, many COTS component suppliers specifically prohibit the use of their components in safety critical applications, in an effort to limit legal responsibility. The responsibility for the acceptable performance of COTS components, in the safety critical application, ultimately falls squarely on the OEM.

The development effort expended by the OEM is the main contributor to the successful application of COTS components in safety critical applications. The development effort, by the OEM, will probably result in a situation where some aspects of the OEMs knowledge and understanding of the COTS component exceeds that of the COTS supplier and the commercial industry in general. However, in order for the OEM to achieve the required assurances with respect to the COTS component, cooperative efforts must be extended by the component supplier: efforts which go beyond the normal commercial component supplier interaction with the customer. The COTS supplier may be motivated to extend cooperative efforts to the OEM, if a financially rewarding opportunity is perceived by the COTS supplier. In some situations, although the COTS supplier is extending cooperative efforts, the COTS supplier is not able to provide the types of assistance or information required by the OEM. In this case, the OEM development effort must be further expanded to develop the required assurances.

6.1 ISSUES AND BARRIERS.

- Design Assurance, Failure Modes, and Component Reliability

  Issue: "Actual availability of COTS component design assurance data as required by DO-254" (see section 11.2.2 of reference 1).

  Issue: It may be difficult to identify all fault modes, i.e., anomalous behavior, for complex COTS components.

  Issue: Actual availability of COTS component data as required to determine failure rates by an Acceptable method.

  Cooperative efforts extended by the COTS component supplier may facilitate the OEM development effort to address these issues; however, in some cases, adequate information may not be available from the COTS supplier. In that case, the OEM will need to reverse-engineer the component to the elemental level required to meet safety objectives, essentially recreating the component to some elemental level. Adequate detailed design information at the elemental level is required to satisfy objectives. This design information may be available from the COTS supplier or a third-party supplier of the elemental item.

  The developmental effort which the OEM is willing to expend in order to adequately assure the COTS component will, in part, determine if the usage is beneficial. In the case of some components and suppliers, the cost benefit ratio may be a barrier.

- Standards

  Issue: Standards for electronics development and production are diverse, do not address the needs of critical systems, and are no longer supported by the federal government.

  The current trend toward performance specifications does not present a barrier to COTS usage, however, adoption of industry standards has historically been an enabler for technology advancement and will continue in the future. Agencies concerned with critical systems should make a concerted effort to influence the standards that are under development in industry.

- Operation Beyond Manufacturer's Specification and Upsets

  Issue: COTS component suppliers discourage use of their components in unintended environments.

  Issue: The manufacturer-specified operating range of COTS components do not meet the requirements for many airborne applications.

  Issue: COTS components may exhibit anomalous behavior due to EMI and radiation.

Operation beyond manufacturer's specification and in the presence of upsets poses a challenge to OEMs which must be addressed through research and development work at the OEM and government/industry-sponsored agencies or consortiums. If certain COTS components are not specifically researched, this may become a barrier to application in airborne systems. Only COTS components, for which OEM or industry-accepted evidence and assurances have been developed, will be incorporated in airborne systems.

- Service Experience

  Issue: The quality of COTS service experience data may be inadequate to meet safety requirements.

  The quality of service experience data may not be adequate to meet safety objectives, however, service experience may provide some level of assurance which can supplement assurances provided by other means. The issue does not present a barrier.

- Configuration Management and Production Practices

  Issue: COTS suppliers are at liberty to change their production processes.

  Issue: COTS suppliers are at liberty to discontinue production of a component resulting in "COTS components which become non-procurable" (see section 11.2.2 of reference 1).

  Issue: "Variations in component parameters that depend on production batches may not be identified, even by robustness tests" (see section 11.2.2 of reference 1).

  Issue: "Evolving aspects of electronic component technology" (see section 11.2.2 of reference 1).

  Issue: Quality control provided by COTS suppliers may be inadequate.

  OEMs can only incorporate COTS components for which adequate assurances and agreements can be obtained from the COTS component supplier. COTS component suppliers who are unwilling to extend this level of cooperative assistance may well present a barrier to the application of their particular components in airborne systems.

  Parts obsolescence poses a significant problem for the OEM, since current mitigation approaches are time/resource consuming and costly. In order to avoid the cost associated with parts obsolescence, OEMs may not adopt new technology until the risk associated with uncertainties is significantly reduced by widespread acceptance in the industry. The parts obsolescence problem therefore delays the adoption of newly developed technology.

- Verification Testing

  Issue: Production testing done by COTS suppliers may fail to detect defective components.

  Issue: OEMs may not have sufficient design information or resources to adequately test complex COTS components.

  The nature of complex electronics does not allow complete testing by deterministic means. As a result, all testing efforts are limited by level of effort and applied resources. The testing required to meet safety system objectives is well beyond accepted commercial practice for COTS components; however, the level of detailed information necessary to establish testing that meets the objectives may not be available to the OEM. Adequate verification testing for complex COTS components is a significant challenge which may present a barrier, unless the OEM system design incorporates design features which can be shown to mitigate failures and anomalous behaviors of the COTS component by other assurance means.

- Role of COTS Tools in Design and Verification

  Issue: Design tools used by both COTS suppliers and OEMs may introduce design errors.

  Issue: Verification tools used by both COTS suppliers and OEMs may fail to identify defective components.

  The development of complex microelectronics is heavily dependent on the use of tools for design and verification. Qualification of the tools to meet objectives for criticality levels A and B was not evidenced in this investigation and may present a barrier to meeting the objectives, unless the development effort required to qualify the tools is undertaken or additional assurance can be gained by other means.

6.2 CONCLUSIONS.

COTS component usage in safety critical applications requires significant OEM development effort targeted at the COTS component and COTS supplier cooperative efforts. While DO-254 treats COTS components as previously designed hardware, the hardware life cycle processes and objectives are applicable to any type of hardware, not precluding COTS usage, but holding all hardware to the same assurance standards. Therefore, while DO-254 objectives do not present barriers to COTS usage, the level of development effort required by the OEM may be cost prohibitive to COTS usage as compared to custom hardware designs. Alternative methods, which attempt to address the issues, are in use throughout the industry; however, the cost of the alternative methods may be prohibitive in many applications.

Levels A and B assurances obviously pose the greatest challenge to the viable use of COTS components due to the development effort required by the OEM to meet assurance objectives.

While the objectives do not constitute barriers, the cost of adequate assurance development may well be a barrier to COTS usage for applications of levels A and B criticality.

The benefits in additional functionality which might be achieved through the use of low-cost COTS components, will be achievable in airborne applications, only if the development effort/cost required for assurances can be secured in a cost-effective manner. Adequate assurances and evidence are achieved at a cost incurred by the OEM and their customers. If the required assurances and evidence, once achieved, could be reused in other applications, the cost could be distributed over a larger population of systems, thus reducing the cost per system. Open systems, reusable designs, and certifiable COTS components with industrywide shared evidence and assurances will be required to gain the functional benefits of COTS components. However, a new paradigm will be required to achieve this in the airborne industry; a central agency, such as the Federal Aviation Administration (FAA), must step up to provide the industry with a centralized source of information on certifiable COTS components and the assurances and evidences which have been achieved. Military specifications, while often criticized, provide standardized methods that are still of great value to industry, despite abandonment by the government. Government- and industry-sponsored consortium, such as CALCE and RAC, are doing research in areas significant to a small segment of military, space, and airborne. OEMs and customers cannot support the entire cost of development for these systems. They must build on and be supported by research, information, and standards made available through central agencies.

7. REFERENCES.

1. Radio Technical Commission for Aeronautics, "Design Assurance for Airborne Electronics Hardware," RTCA DO-254/EUROCAE ED-80, April 19, 2000.

2. Pecht, M., J. Boullie, E. Hakim, A. Jain, M. Jackson, I. Knowles, R. Shroeder, A. Strange, and J. Wyler, "The Realism of FAA Reliability-Safety Requirements and Alternatives," *IEEE AES Systems Magazine*, February 1998.

3. Duncan Young, "From Avionics to Vetronics: Considerations for Application of COTS VME to Deployed Defense Systems," DY 4 Systems, http://www.dy4.com/cots/position.htm.

4. Krinke, T.A. and D.K. Pai, "COTS/ROTS for Mission-Critical Systems," General Dynamics Information Systems.

5. "Team Submarine Strategy 2000 Commercial-Off-The-Shelf (COTS) Acquisition Primer," 12 November 1996 http://pats.crane.navy.mil/pubdoc/cotsacqu.doc.

6. *"Critical IC Roadmap,"* Sandia National Laboratory, 1998, http://www.sandia.gov/eqrc/critical/cicroadm.pdf.

7. Susan Scheck, "COTS Initiatives Save Military OEMs Millions," *Electronic Buyers' News,* February 19, 1999 (1:48 PM) URL: http://www.ebnews.com/story/OEG19990219S0048.

8. Dellin, T.A., J.L. Jorgensen, P.S. Winokur, and A.D. Romig, Jr., "New Trends in the Commercial IC Industry and the Impact on Defense Electronics," Sandia National Laboratories, 1998.

9. "Overcoming Barriers to the Use of Commercial Integrated Circuit Technology in Defense Systems," October 1996, http://www.acq.osd.mil/es/dut/ic/contents.htm.

10. Defense MicroElectronics Activity (DMEA) DMSMS Overview," http://www.dmea.osd.mil/dmsms_overview.html.

11. Dr. Ted Dellin, "Economic and Silicon Trends in the Commercial Industry and Their Impact on ICs Used in Critical Applications," Electronics Quality/Reliability Center Sandia National Laboratories, Albuquerque, NM, http://www.sandia.gov/eqrc/critical/critico3.pdf.

12. Ted Dellin, "Critical IC Applications Community," Sandia National Laboratories, http://www.sandia.gov/eqrc/critical/cicappl.pdf.

13. Low Volume Critical Electronics, web book, CALCE Electronic Products and Systems Center, http://www.calce.umd.edu/.

14. Connie S. Beane, "Use of Integrated Circuits in Commercial Aviation, Federal Aviation Administration Transport Airplane Directorate, http://www.sandia.gov/eqrc/critical/beane.pdf.

15. Brent Meyer, "Integrated Circuits in Nuclear Weapon Applications," Sandia National Laboratories, Digital Microelectronics Department, November 11, 1997, http://www.sandia.gov/eqrc/critical/meyer.pdf.

16. "Space Industry Steers Satellite Designs to COTS," *EE Times*, November 9, 1999 (11:20 AM) URL: http://www.eetimes.com/story/OEG 19991119S0021.

17. G.E. Servais, "Criteria for Critical Integrated Circuits," Delco, http://www.sandia.gov/eqrc/critical/servais.pdf.

18. Ron Kalin and Dennis Scranton, "Reliability of Life Support Medical Electronics," Sandia National Laboratories Electronics Quality/Reliability Center, http://www.sandia.gov/eqrc/critical/kalin.pdf.

19. Jonathan F. Luedeke, "Safety of High Speed Guided Ground Transportation Systems, Analytical Methodology for Safety Validation of Computer Controlled Subsystems, Volume I: State of the Art and Assessment of Safety Verification/Validation Methodologies," Battelle, DOT/FRA/ORD-95/10.1||DOT/VNTSC-FRA-95-8.I NTIS#: PB96-109772, September 1995.

20. Jonathan F. Luedeke, "Safety of High Speed Guided Ground Transportation Systems, Analytical Methodology for Safety Validation of Computer Controlled Subsystems, Volume II: Development of a Safety Validation Methodology," Battelle,

DOT/FRA/ORD-95/10.2||DOT/VNTSC-FRA-95-8.II||NTIS#: PB96-109780, September 1995.

21. Virtual Socket Interface (VSI) Alliance, http://www.vsi.org/index.htm.

22. Dr. Wayne L. O'Hern, Jr., Task Force Chairman, "An Open Systems Process for DoD: FINAL REPORT," DSB Task Force on Open Systems (OSTF), 25 September 1998.

23. George Leopold, "DoD Questioned on Off-the-Shelf Technology Tack," http://www.eet.com/news/97/939news/dodquest.html.

24. Maurice Klapfish, "U.S. Bus Usage Trends in Major Applications," Exhibit 5, http://www.busandboard.com/proceedings/pdfs/vdc.pdf.

25. David Lieberman, "Board Makers Find New Market in COTS," *EE Times,* December 2, 1998(12:00PM), http://www.eetimes.com/story/OEG19981202S0004.

26. Lynn M. Patterson, "Deploying Commercial-Off-The-Shelf Digital Signal Processing Technology," VP Product Development, Ixthos, Inc., http://www.ixthos.com/technical/notes_articles/articles/COTS%20DSP.html.

27. Radstone Technology, http://www.radstone.com/buildlevels.html.

28. DY 4 Systems Inc., http://www.dy4.com/Experience/RuggLevels.htm.

29. Vista Controls Corp., http://www.vistacontrols.com/.

30. "Motorola Introduces PowerPC 603eTM Microprocessors at Extended Temperatures," http://www.mot.com/SPS/PowerPC/library/press_releases/603extemppr.html.

31. Leopold, G. and Craig Matsumoto, "Intel Discharges Its MIL-Spec ICs, *EE Times.com* (EDTN Network) http://www.eet.com/news/97/938news/milspec.html.

32. "Cypress Semiconductor," Cypress Military, http://www.cypress.com/military/index.html and Design Resources http://www.cypress.com/design/quality/awards.html.

33. "Testing and Burn-in of Actel FPGAs," found under Aerospace Application Notes, http://www.actel.com/support/appnotes.

34. "Xilinx, Los Alamos National Laboratory Team Up on Space-Based Reconfigurable Data Processing," http://www.xilinx.com/prs_rls/2005.htm.

35. "Next Generation of Electronics for United Airlines New 777," National Semiconductor Corporation, http://www.national.com/news/1995/9505/corp95006misc.html.

36. Rochester Electronics, company web page, http://www.rocelec.com/.

37. "Honeywell Commercial Avionics Electronics Overview," Honeywell Solid State Electronics Center, http://www.ssec.honeywell.com/avionics/index.html.

38. "Suppliers Urging More Integration of Third-Party IP Designs," ebn (EDTN Network), http://www.ebns.com/topsemi99/1153asic.html.

39. Rodney Myrvaagnes, "Programmable Logic Expands Capacity and Variety, http://electronicproducts.com/ShowPage1.asp?SECTION=&PRIMID=&FileName=FEBPLD1%2EFEB2000&ReturnLink=%2FSearch1%2Easp%3FManufacturer%3D%26Keyword%3DFPGA%26Category%3DProgrammable%2BLogic%26StartNum%3D1%26year%3D1&MonthYear=Feb+2000.

40. Rick Nordin, "IP Core Characterization and Static Timing Verification," http://www.synopsys.com/products/etg/coremill_wp.html.

41. "IEEE Guide for Selecting and Using Reliability Predictions Based on IEEE 1413," http://www.manta.ieee.org/groups/reliability/wg1413/Rel_Pred_Guide1199.doc.

42. Ned H. Criscimagna, "Benchmarking Commercial Reliability Practices," Reliability Analysis Center, July 1995.

43. *Journal of the Reliability Analysis Center*, Third quarter 1999.

44. Ned H. Criscimagna, "Evaluating the Reliability of Commercial-Off-The-Shelf (COTS) Items," Reliability Analysis Center, August 1999.

45. Billy M. DeBusk Jr., "Managing the Reliability of COTS-Based Military Systems," Northrop Grumman, Proceedings of Annual Reliability and Maintainability Symposium, 1998, p. 394.

46. Paul V. Dressendorfer, "Packaging Trends: Using Integrated Circuits in Critical Applications Workshop," Sandia National Laboratories http://www.sandia.gov/eqrc/critical/dressendorfer.pdf.

47. "Collection and Categorisation of Worldwide Standards Relevant to the Use of Programmable Electronic Systems in Safety Related Applications," http://ntsta.jrc.it/dsa/sccs-dir/std.htm.

48. M. Pecht, J. Fink, E. Hakim, and J. Wyler, "An Assessment of the Qualified Manufacturer List (QML)," *IEEE Aerospace and Electronic Systems,* Vol. 12, No. 7, July 1997, pp. 39-43.

49. Richard E. Anderson, "Failure Analysis Challenges for Sub 0.25 μm Technologies," Sandia National Laboratories, http://www.sandia.gov/eqrc/critical/anderson.pdf.

50. Integra Technologies L.L.C., http://www.cetc.com/intel.html.

51. Normand, Eugene, "Single-Event Effects in Avionics," (Boeing Defense and Space Group) *IEEE Transactions on Nuclear Science,* Vol. 43, Issue 2, Pt. 1, April 1, 1996, pp. 461-474.

52. Charles Barnes and Allan Johnston, "Recent Radiation Effects Activities at JPL: Coping With COTS," Noordivijk, the Netherlands, April 21-25, 1997.

53. C.I. Lee, B.G. Rax, and A.H. Johnston, "Hardness Assurance Techniques for New Generation COTS Devices," Jet Propulsion Laboratory Technical Report, Indian Wells, California, USA, July 15-19, 1996.

54. Kinnison, James D., "Single Event Phenomena: Testing and Prediction," (Johns Hopkins Univ.) Idaho Univ., The 1992 4th NASA SERC Symposium on VLSI Design January 1, 1992, p. 11.

55. Karp, Sherman and Gilbert, Barry K., "Digital System Design in the Presence of Single Event Upsets," (Mayo Clinic) *IEEE Transactions on Aerospace and Electronic Systems,* Vol. 29 Issue 2, April 1, 1993, pp. 310-316.

56. Turflinger, Thomas L. and Davey, Martin V., "Understanding Single Event Phenomena in Complex Analog and Digital Integrated Circuits," (U.S. Navy, Naval Weapons Support Center) *IEEE Transactions on Nuclear Science,* Vol. 37, December 1, 1990, pp. 1832-183.

57. Taber, A. (IBM Federal Systems Co.) and Normand, E. (Boeing Defense and Space Group), "Single Event Upset in Avionics," *IEEE Transactions on Nuclear Science,* Vol. 40, Issue 2, April 01, 1993, pp. 120-126.

58. "Minimizing Single Event Upset Effects Using Synopsys," found under Aerospace Application Notes at http://www.actel.com/support/appnotes.

59. "Using Synplify to Design in Actel Radiation-Hardened FPGAs," Actel Aerospace http://www.actel.com/appnotes/SynplifyRH.pdf.

60. Dr. Gary L. Fitzhugh, "Reconfigurable Logic Engines—A Solution to Electronic Systems Obsolescence," Visicom Laboratories, Inc., Alexandria, Va., July 1997.

61. Keith Bergevin, "Redesign and Testing of Obsolete ASICs," Defense Micro Electronics Activity (DMEA), http://smaplab.ri.uah.edu/dmsms98/presentations/lau.pdf.

62. Ryan L. Badger "Analyzing and Verifying Complex System-on-a-Chip Designs," Embedded Systems Conference, San Jose, CA, September 28, 1999.

63. Terry Strickland, "Design-for-Test Methodologies and Tools for ASIC Design; An Array of DFT Solutions Offers a Range of Capabilities," http://electronicproducts.com/ShowPage1.asp?SECTION=&PRIMID=70091&FileName=COMPASS%2EJUN1995&Manufact=Compass+Design+Automation&ReturnLink=%2FSearch1%2Easp%3FManufacturer%3D%26Keyword%3DDesign%252Dfor%252Dtest%2Bmethodologies%2Band%2Btools%2Bfor%2BASIC%2Bdesign%26Category%3DAll%26StartNum%3D1%26year%3D5&MonthYear=Jun+1995.

64. Jim Lipman, "Add Testability NOW to Core-Based Chips, OR Pay Later," February 16, 1998, http://www.ednmag.com/reg/1998/ 021698/04df_01.htm.

65. Edward I. Cole Jr., Jerry M. Soden, Paiboon Tangyunyong, Patrick L. Candelaria, Richard W. Beegle, Daniel L. Barton, Christopher L. Henderson, and Charles F. Hawkins, "Transient Power Supply Voltage (v DDT) Analysis for Detecting Defects," Electronics Quality/Reliability Center, http://www.sandia.gov/eqrc/critical/cole.pdf.

66. L. Harrison and B. Landell, "Digital Systems Validation Handbook, Volume III, Design, Test, and Certification Issues for Complex Integrated Circuits—Chapter 2," DOT/FAA/AR-95/125-III,2, July 1996.

67. L. Harrison and B. Landell, "Design, Test, and Certification Issues for Complex Integrated Circuits," DOT/FAA/AR-95/31, August 1996.

68. K. Cluff, D. Barker, D. Robbins, and T. Edwards, "Characterizing the Commercial Avionics Thermal Environment for Field Reliability Assessment," *Proceedings-Institute of Environmental Sciences*, 1996, pp. 50-57.

69. J. Jordan, M. Pecht, and J. Fink, "How Burn-In Can Reduce Quality and Reliability," *The International Journal of Microcircuits and Electronic Packaging*, Vol. 20, No. 1, 1997, pp. 36-40, First Quarter.

70. Reza Ghaffarian, "Reliability of BGA Packages for Highly Reliable Application and Chip Scale Package Board Level Reliability," San Jose, California, USA, September 1997.

71. "Guidance for the Adoption of Tools for Use in Safety Related Software Development," British Computer Society, Institution of Electrical Engineers, http://www.iee.org.uk/ PAB/SCS/tools.html.

72. Rowan L. Dordick, "A Chip Verification on a Large Scale," IBM.

73. "Design VERIFYer," Avanti Corporation, http://www.avanticorp.com/product.

74. Jim Lipman, "Chip Verification: A Formal Affair?" http://www.ednmag.com/reg/1998/ 010198/01df_02.htm.

75. Clive Maxfield, "Whose Fault is it Anyway? An Introduction to Digital Fault Simulation," http://www.ednmag.com/reg/1996/060696/12df3.htm.

76. Jim Lipman, "Postlayout EDA Tools Lock Onto Full-Chip Verification," http://www. ednmag.com/reg/1996/101096/21df_03.htm.

77. "New Tools and Methods Flourish at the Design Automation Conference," *Electronic Products*, http://electronicproducts.com/ShowPage1.asp?SECTION=&PRIMID=&File Name=JUNOL2%2EJUN1999&ReturnLink=%2FSearch1%2Easp%3FManufacturer%3

D%26Keyword%3Dtools%252C%2Bautomation%2Bconference%26Category%3DAll%26StartNum%3D61%26year%3D1&MonthYear=Jun+1999.

78. "The Roll of EDA in the Electronics Industry," Business Section of Synopsys Corporate, http://www.synopsys.com/corporate/invest/annual10k99/part1_10k99.html.

79. Simon Young, "Scaling the Nanometer Wall With Reliability Analysis and Verification," Synopsys, Inc., January 1999 http://www.synopsys.com/products/etg/reliability_wp.html.

80. "Electronic Design Automation," Linda Geppert, *IEEE Spectrum*, January 2000.

81. "Avionics Industry: Guide for Reliability Assessment of Electronics Equipment" International Electrotechnical Commission, Report # QC 001007-1-3: 2000.

82. Part Requirement and Application Manual, Naval Sea Systems Command Report Number TE000-AB-GTP-010 revision 2, http://pats.crane.navy.mil/component/applications.htm.

83. M. Pecht, A. Shukla, N. Kelkar and J. Pecht, "Criteria for the Assessment of Reliability Models," *IEEE Transactions on Components, Packaging, and Manufacturing Technology-Part B*, Vol. 20, No. 3, August, 1997, pp. 229-234.

84. Y Zhang, et al, "Trends in Component Reliability and Testing, Semiconductor International, September 1999.

85. "Avionics Industry: Guide for Using Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges," International Electrotechnical Commission, Report # QC 001007-1-2: 2000.

86. "Stress Balancing: A Method for Use of Electronic Parts Outside the Manufacturer Specified Temperature Range," CALCE, 1999.

87. "Obsolescence: The Dark Little Secret of COTS, Military and Aerospace Electronics," February 1999

88. Dan Strassberg, "BIST and ATE Team to Tame IC-Test Cost," EDN http://www.ednmag.com/ednmag/reg/2000/03022000/Volume45-Issue05.asp .

8. RELATED RESOURCES.

United Technologies Research Center, Krodel, J., "Commercial-Off-The-Shelf (COTS) Avionics Software Study," DOT/FAA/AR-01/26, May 2001.

http://eis.jpl.nasa.gov/quality/Formal_Methods/
"Formal Methods Specification and Analysis Guidebook for the Verification of Software and Computer Systems, Volume II: A Practitioner's Companion" [NASA-GB-001-97], 1997, 245 pages.

http://www.aiaa.org/
The nonprofit American Institute of Aeronautics and Astronautics (AIAA) is the principal society and voice serving the aerospace profession. Its primary purpose is to advance the arts, sciences, and technology of aeronautics and astronautics, and to foster and promote the professionalism of those engaged in these pursuits.

http://www.air-transport.org/
The ATA is the Air Transport Association of America. Founded by a group of 14 airlines meeting in Chicago in 1936, it was the first, and today remains, the only trade organization for the principal U.S. airlines. The purpose of the ATA is to support and assist its members by promoting the air transport industry and the safety, cost-effectiveness, and technological advancement of its operations; advocating common industry positions before state and local governments; conducting designated industrywide programs; and assuring governmental and public understanding of all aspects of air transport.

http://www.arinc.com/Ind_Govt_Srv/AEEC/aeec.html
The Airlines Electronic Engineering Committee (AEEC) is an international body of airline representatives. AEEC sets the standards for avionics equipment used on the world's commercial air transport aircraft. Over 5000 engineers and scientists representing nearly 500 organizations participate in the AEEC standards setting process. AEEC standards are coordinated with many airline organizations including the International Civil Aviation Organization (ICAO).

http://www.aviationsafetyalliance.org
The Aviation Safety Alliance is a 501(c)(6) advocacy organization dedicated to educating the media and the general public about aviation safety. The affiliated 501(c)(3) Aviation Safety Alliance Education Fund allows the Alliance to provide informative seminars and other programs.

http://www.aviationnow.com/TwoShare/getPage/AWContent/AWST/awst_main_awstheadlines
Welcome to Aviation Week's AviationNow.com, the premiere online professional resource for people in the aviation and aerospace industry. AviationNow.com will change the global aviation and aerospace community and the way we communicate with real-time news, features and data resources, plus unique services and e-business utilities designed to help industry professionals become better connected in the worldwide aviation and aerospace marketplace.

http://www.bmpcoe.org/index.html
The Best Manufacturing Practices (BMP) program has changed American industry's cultural bias by sharing information with other companies, including competitors. This unique, innovative, technology transfer program is committed to strengthening the U.S. industrial base. The main goal of BMP is to increase the quality, reliability, and maintainability of goods produced by American firms. The primary steps toward this goal are simple: identify best practices, document them, and then encourage industry, government, and academia to share information about them. The BMP program, sponsored by the Office of Naval Research, enables the U.S. defense industrial base to lower acquisition cost and improve product price, quality, and delivery.

http://www.calce.umd.edu/
CALCE is a consortium of the world's leading avionics, automotive, computer, semiconductor, and electronics manufacturers. It represents a successful international industry-government-academic partnership. The Consortium provides information and services that match industry needs and provides an organizational structure by which different sectors of the electronics industry supply chain can share information and influence practices and policies.

http://www.casi.ca/
The Canadian Aeronautics and Space Institute (CASI) is a nonprofit scientific and technical organization for aerospace professionals. CASI was created to advance the art, science, engineering, and application of aeronautics and space in Canada. Today, the Institute is a focal point for communications among members of the aeronautics and space community. CASI is also a strong voice for research and development, and supports science and engineering education in Canada.

http://www.acq.osd.mil/es/dut/
Commercial Operations and Support Savings Initiative (COSSI) is a joint program of the U.S. Army, U.S. Navy, and U.S. Air Force with oversight administration by the Office of Secretary of Defense. COSSI's mission is to develop and test a method for reducing Department of Defense (DoD) Operations and Support (O&S) costs by routinely inserting commercial items into fielded military systems.

http://www.sandia.gov/eqrc/critical/critical.html#TOP
The Critical IC Workshop and Roadmap (CRITICAL) addresses the synergistic needs of the various applications that use integrated circuits (IC) in applications with high consequences of failure.

http://www.dmsnews.com/about.html
DMS NEWS and COTS REPORT is an electronics newsletter and information service with news, research, case studies, and comment for engineers, executives and all professionals in the aerospace, defense, transportation, computers, electronics, and telecommunications industries.

http://www.ee.duke.edu/~ssg/softrel/project.html
Center for Advanced Computing and Communication, Duke University, Software Reliability and Performance.

https://auth.cahners.net/edn/FormsLogin.asp?/edn/GetInfo.asp?RA_Pers=yes&RA_Domain=www.ednmag.com&RA_S=off&RA_Script=SetInfo.asp&RA_Return=/ednmag/reg/search.asp
Electronic Design News (EDN). Welcome to the Archives of *EDN* magazine. Search by topic, technology, manufacturer or key word to find past articles of *EDN*.

http://www.empf.org/html/empfset.htm
The EMPF was established by the U.S. Navy in 1984 in Ridgecrest, California, with a mandate to team with industry to develop, test, and analyze state-of-the-art electronics manufacturing processes and electronics production equipment. The goal of the EMPF and its partners in industry was, and is, to achieve consistent production of reliable products for the nation's

defense by promoting the use of efficient and cost-effective manufacturing processes and equipment.

http://electronicproducts.com/ep.asp
Search Electronic Products magazine. Search our online database by product category, manufacturer, or keyword for every product and feature run in the print version of the magazine.

http://www.embedded.com/
Embedded Systems Programming is a monthly magazine devoted to engineers, programmers, and project leaders who build microcontroller and embedded microprocessor-based systems.

http://www.cnde.iastate.edu/casr.html
The FAA Center for Aviation Systems Reliability (FAA-CASR) has the following objectives: (1) To provide quantitative NDE techniques, procedures, and prototypes that assure the airworthiness and reliability of aviation systems and (2) to provide comprehensive education and training tools for the FAA, airlines, and manufacturers on aviation specific NDE technologies.

http://www.csl.sri.com/sri-csl-fm.html
SRI International Computer Science Laboratory Formal Methods and Dependable Systems

http://www.fmeurope.org
Formal Methods Europe (FME) is a European organization supported by the Commission of the European Union (via ESSI of the ESPRIT programme), with the mission of promoting and supporting the industrial use of formal methods for computer systems development.

http://www.cs.ubc.ca/formalWARE/welcome.htm
*formal*WARE was a two-year collaborative industry/university research project. This project was funded to investigate potential applications of formal methods in the development of software-intensive, critical systems. The research scope of this project included requirements specification and validation; requirements-based, system level testing; software component engineering; and system safety engineering.

http://www.seas.gwu.edu/~irra/work-frame.html
The Institute for Reliability and Risk Analysis (IRRA) was founded in 1981 to initiate basic and applied research aimed toward increasing the fundamental knowledge base and methodology in reliability, warranties, quality control, and risk analysis.

http://www.hiten.com/guests/categories/AERO.html
The High Temperature Electronics Network (HITEN) is the world's leading source of technical and strategic business information on high-temperature electronics and related technologies.

http://www.iecq.org/_private/AWG.htm
The Avionics Working Group (AWG) was set up during the IECQ-CMC meeting in Houston, 1998 on October 15-16. Mission is to develop and maintain industry procedures for electronic component management in the avionics industry. Tasks: form the working group, identify

documents needed for electronic component management, extended temperature range, and reliability assessment.

http://www.iee.org.uk/PAB/SCS/scs_pub.htm
The Institution of Electrical Engineers, Safety Critical Publications.

http://www.itea.org/
The International Test and Evaluation Association (ITEA), is a not-for-profit educational organization founded in 1980 to further the exchange of technical information in the field of test and evaluation. Its members include professionals from industry, government, and academia who are involved in the development and application of policy and techniques used to assess the effectiveness, reliability, and safety of new and existing systems and products.

http://www.milaero.com/
Military & Aerospace Electronics: The Technology News Publication of Mil-Spec, High-Rel, Rugged, and COTS Design.

http://rac.iitri.org/
The Reliability Analysis Center (RAC) is a DoD Information Analysis Center (IAC). RAC's scope is the reliability, maintainability, quality, and supportability of microcircuits, semiconductors, electromechanical and mechanical parts, and equipment/systems employing these parts. IIT Research Institute (IITRI) has operated the RAC since its inception in 1968.

http://www.enre.umd.edu//enreumd.htm
Reliability Engineering Center at the University of Maryland.

http://catless.ncl.ac.uk/Risks
Forum on risks to the public in computers and related systems. ACM Committee on Computers and Public Policy.

http://www.rtca.org/default.htm
Radio Technical Commission for Aeronautics (RTCA), Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. RTCA functions as a federal advisory committee. Its recommendations are used by the Federal Aviation Administration (FAA) as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment, and other business decisions.

http://ntsta.jrc.it/dsa/sccs-dir/index.htm
JRC Dependable Software Applications: To be an impartial center of expertise in dependable systems that are safety, mission, security or environmentally critical, or whose failure could lead to large economic losses. Aims to accomplish this by providing support to European policy in the field of Information Society Dependability and by developing and transferring dependability technologies.

http://www.sandia.gov/eqrc/home.html
Revolutionizing electronics reliability, failure analysis, defect detection, and vulnerability assessment is the mission of Sandia's Electronics Quality/Reliability Center (EQRC). The EQRC's award winning technical solutions not only meet the needs of Sandia's critical missions, they are being used today by a broad base of leading commercial electronics manufacturers.

http://www.sei.cmu.edu/topics/about/about.html
The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense through the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD (AT&L)]. The SEI contract was competitively awarded to Carnegie Mellon University in December 1984. The SEI mission is to provide leadership in advancing the state of the practice of software engineering to improve the quality of systems that depend on software.

http://www.sematech.org/public/index.htm
International SEMATECH is a unique endeavor of 13 semiconductor manufacturing companies from seven countries. Located in Austin, Texas, USA, the consortium strives to be the most effective, global consortium influencing semiconductor manufacturing technology.

http://www.semichips.org/
The Semiconductor Industry Association is the leading trade association representing the computer chip industry. The mission of the SIA is to provide leadership for U.S. chip manufacturers on the critical issues of trade, technology, environmental protection, and worker safety and health.

http://www.stackinternational.com/a_frame.htm
STACK International is a group of multinational, independent electronic equipment manufacturers who share experience, "know how," workload and co-operate in *precompetitive* areas with each other and their suppliers to reduce individual members' cost and risk of component ownership.

http://telecom-info.telcordia.com/site-cgi/ido/index.html
Bellcore is now Telcordia Technologies. Standards documents.

http://www.vsi.org/index.htm
Virtual Socket Interface Alliance (VSIA) was formed in September 1996 with the goal of establishing a unifying vision for the system-chip industry and the technical standards required to enable the most critical component of the vision; the mix and match of Virtual Components (IP) from multiple sources. The VSIA vision is to dramatically accelerate system chip development by specifying open standards that facilitate the mix and match of Virtual Components from multiple sources.

GOVERNMENT INITIATIVES

http://www.faa.gov/avr/air/airhome.htm
The Aircraft Certification Service is responsible for the safety of civil aircraft. The inherent safety of an aircraft is a function of its design integrity and its manufacturing quality. It is the mission of the Aircraft Certification Service to promote safety by: prescribing safety standards governing the design, production quality, and airworthiness of civil aeronautical products; administering design, production quality, and finished product certification programs in compliance with the prescribed safety standards; monitoring safety performance and acting to provide continued operational safety of aircraft.

http://av-info.faa.gov/software/
Aircraft Certification Service Software home page.

http://cots.jpl.nasa.gov/
The focus of the Commercial Off-The-Shelf (COTS) Parts/Technology Program is the infusion of commercial grade state-of-the-art parts into JPL hardware and systems. It is supported by the JPL Technical Infrastructure Program. The performance, reliability, and quality of COTS parts should meet the requirements of the mission they are used in.

http://www.faa.gov/search.htm

http://www.faa.gov/avr/AFS/FARS/far_idx.htm
Title 14 Code of Federal Regulations (CFR), Chapters I and III, Federal Aviation Regulations

http://www.gidep.org/rm/rmlinks.htm
Government Industry Data Exchange program (GIDEP) R&M Related Sites

http://theory.stanford.edu/~sipma/
Henny Sipma. Research associate at the Computer Science Department at Stanford University. Works with Zohar Manna on the specification and verification of reactive systems. Research Interests: specification and verification of real-time and hybrid systems, visual formalisms for verification, combining model checking and deduction, application of verification methods to PLC's (programmable logic controllers), and industrial safety systems (such as emergency shutdown systems in chemical plants and refineries).

http://www.jedec.org/
The JEDEC Solid State Technology Association (Once known as the Joint Electron Device Engineering Council) is the semiconductor engineering standardization body of the Electronic Industries Alliance (EIA), a trade association that represents all areas of the electronics industry.

http://eeeparts.jpl.nasa.gov/
The EEE Parts Program at JPL is a technology evaluation and assessment program, where new and emerging microelectronics technologies are evaluated for space applications. The selection process of the specific topics for technology evaluation involves continuous interaction between the program personnel and the various NASA, industry, and other technology development leaders.

http://techreports.jpl.nasa.gov/
The Jet Propulsion Laboratory Technical Report Server is a database of Abstracts, Citations, and full text Technical Reports written by and for the scientific and technical community.

http://shemesh.larc.nasa.gov/fm/fm-quick.shtml
NASA Langley Formal Methods Team

http://techreports.larc.nasa.gov/cgi-bin/NTRS
The NASA Technical Report Server is an experimental service that allows users to search the many different abstract and technical report servers maintained by various NASA centers and programs. Specifically, it is a unified interface to many separate WAIS servers. NTRS is both a superset of the of the various servers and a canonical listing of the servers.

http://www.acq.osd.mil/osjtf/
The Open Systems Joint Task Force (OS-JTF) was formed in September 1994 to: "Sponsor and accelerate the adoption of open systems in weapons systems and subsystems electronics to reduce life-cycle cost and facilitate effective weapon system intra- and interoperability."

OTHER LINK COLLECTIONS

http://www.militaryelectronics.com/index.html
Welcome to the Electronics Resource Center, the WWW connection that links users and providers together at a single point of access for both technical and purchasing information.

http://www.asq-rd.org/links.htm
American Society for Quality, Reliability Division – Links

http://www.si2.org/cfi/EDA-WWW.html
SI2, Inc. is an international, not-for-profit consortium of CAD (computer-aided design) tool users, tool vendors, and research institutions. Since 1988, SI2's mission is to provide industry-accepted standards and technology that enable interoperability of electronic design automation (EDA) applications and data for end-users and suppliers worldwide.

http://pats.crane.navy.mil/pub.htm#cots
PATS (Product and Technology Surveillance) is a shared knowledge-based Internet used to compile and distribute market survey and technology trending information and support COTS product selection decisions.

http://cmmr.crane.navy.mil/cmmr2.htm
Commercial item Military Market Research Information Center (CMMR)

http://rac.iitri.org/InfoResources/Rac_WebSites.html
RAC related web sites.

http://www-osat.grc.nasa.gov/
The NASA Glenn Research Center (GRC) Office of Safety and Assurance Technologies (OSAT) provides reliability, quality assurance, and system safety management and expertise to support the Glenn Research Center technical divisions, project offices, and contracted programs—Safety, Reliability, and Quality Resources.

http://www.cs.ubc.ca/formalWARE/safety.htm#safety_refs
FormalWARE Publications and Presentations

http://archive.comlab.ox.ac.uk/safety.html
Pointers to information on Safety-Critical Systems

http://www.acq.osd.mil/es/dut/ic/contents.htm
Overcoming Barriers to the Use of Commercial Integrated Circuit Technology in Defense Systems, October 1996.

http://www.nap.edu/readingroom/books/defman/es.html
Defense Manufacturing in 2010 and Beyond Meeting the Changing Needs of National Defense: Committee on Defense Manufacturing in 2010 and Beyond; Board on Manufacturing and Engineering Design Commission on Engineering and Technical Systems; National Research Council.

http://bob.nap.edu/html/airworthiness/
Improving the Continued Airworthiness of Civil Aircraft—A Strategy for the FAA's Aircraft Certification Service.

http://eis.jpl.nasa.gov/quality/Formal_Methods/
NASA Formal Methods Guidebook, Vol. I, Release 2.0

http://www.iplbath.com/p80.htm
Papers from IPL on software testing.

http://www.dscc.dla.mil/Programs/MilSpec/listDocs.asp?BasicDoc=MIL-STD-883
MIL-STD-883 Test Methods and Procedures for Microelectronics

http://www.sandia.gov/eqrc/critical/cictalks.html
Workshop Presentations—Using ICs in Critical Applications Workshop and Roadmap